

[H.A.S.C. No. 111-77]

**CHALLENGES TO EFFECTIVE
ACQUISITION AND MANAGEMENT OF
INFORMATION TECHNOLOGY SYSTEMS**

HEARING

BEFORE THE

PANEL ON DEFENSE ACQUISITION REFORM

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

HEARING HELD
JULY 9, 2009



**CHALLENGES TO EFFECTIVE ACQUISITION AND MANAGEMENT OF
INFORMATION TECHNOLOGY SYSTEMS**

[H.A.S.C. No. 111-77]

**CHALLENGES TO EFFECTIVE
ACQUISITION AND MANAGEMENT OF
INFORMATION TECHNOLOGY SYSTEMS**

HEARING

BEFORE THE

PANEL ON DEFENSE ACQUISITION REFORM

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

HEARING HELD

JULY 9, 2009



U.S. GOVERNMENT PRINTING OFFICE

51-959

WASHINGTON : 2010

PANEL ON DEFENSE ACQUISITION REFORM

ROBERT ANDREWS, *New Jersey, Chairman*

JIM COOPER, *Tennessee*

K. MICHAEL CONAWAY, *Texas*

BRAD ELLSWORTH, *Indiana*

DUNCAN HUNTER, *California*

JOE SESTAK, *Pennsylvania*

MIKE COFFMAN, *Colorado*

KEVIN GATES, *Professional Staff Member*

JOHN WASON, *Professional Staff Member*

ALICIA HALEY, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2009

	Page
HEARING:	
Thursday, July 9, 2009, Challenges to Effective Acquisition and Management of Information Technology Systems	1
APPENDIX:	
Thursday, July 9, 2009	25

THURSDAY, JULY 9, 2009

CHALLENGES TO EFFECTIVE ACQUISITION AND MANAGEMENT OF INFORMATION TECHNOLOGY SYSTEMS

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Andrews, Hon. Robert, a Representative from New Jersey, Chairman, Panel on Defense Acquisition Reform	1
Conaway, Hon. K. Michael, a Representative from Texas, Ranking Member, Panel on Defense Acquisition Reform	3

WITNESSES

Harp, Timothy J., Deputy Assistant Secretary of Defense, Command, Control, Communications, Intelligence, Surveillance, Reconnaissance and Information Technology Acquisition, Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer ...	5
Kerber, Dr. Ronald L., Co-Chair, Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology	9
Nielsen, Dr. Paul D., Director and Chief Executive Officer, Software Engineering Institute, Carnegie Mellon	7

APPENDIX

PREPARED STATEMENTS:	
Andrews, Hon. Robert	29
Conaway, Hon. K. Michael	30
Harp, Timothy J.	34
Kerber, Dr. Ronald L.	62
Nielsen, Dr. Paul D.	48
DOCUMENTS SUBMITTED FOR THE RECORD:	
Defense Science Board 2006 Summer Study on Information Management for Net-Centric Operations, Volume I, Main Report, April 2007	234
Defense Science Board 2006 Summer Study on Information Management for Net-Centric Operations, Volume II, Operations Panel Report, April 2007	352
Report of the Defense Science Board: Creating a DOD Strategic Acquisition Platform, April 2009	87

IV

	Page
DOCUMENTS SUBMITTED FOR THE RECORD—Continued	
Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology, March 2009	133
WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING: [There were no Questions submitted during the hearing.]	
QUESTIONS SUBMITTED BY MEMBERS POST HEARING:	
Mr. Andrews	433

CHALLENGES TO EFFECTIVE ACQUISITION AND MANAGEMENT OF INFORMATION TECHNOLOGY SYSTEMS

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
PANEL ON DEFENSE ACQUISITION REFORM,
Washington, DC, Thursday, July 9, 2009.

The panel met, pursuant to call, at 8:00 a.m., in room 2212, Rayburn House Office Building, Hon. Robert Andrews (chairman of the panel) presiding.

OPENING STATEMENT OF HON. ROBERT ANDREWS, A REPRESENTATIVE FROM NEW JERSEY, CHAIRMAN, PANEL ON DEFENSE ACQUISITION REFORM

Mr. ANDREWS. We are very happy to have you with us this morning. The witnesses have done a really good job preparing their written testimony. We look forward to hearing them elaborate on that testimony this morning so we can learn more. The panel is focused on the difference, if any, that exists between cost and value for our uniformed personnel, their support personnel, and the taxpayers of the country.

We spend an enormous amount of money in the defense of our country, and we should. It is our responsibility to make sure that that money is spent prudently and wisely, so those who step forward to defend our country have the best technology available, the best tools available to do their jobs for our country so that the taxpayers are receiving full and robust value for their investment in the defense of the country.

The panel's work project has proceeded in several steps. We had begun with the question of whether there are adequate metrics to measure the difference, if any, between cost and value. We are now proceeding in a second mode of analysis, which deals with hypotheses about why differences between cost and value have emerged. The third section of our inquiry will deal with proposed solutions to deal with those problems. Then, finally, the panel will convene toward the end of our term and come up with recommendations, which we look forward to advocating in the fiscal year 2011 armed services authorization bill.

This morning, we are going to focus on a critical hypothesis about the difference between cost and value, and that is the inadequacies through which the United States Department of Defense (DOD) purchases information technology (IT) and the challenges that we face in doing that. This is sort of a collision of two cultures, as I see it.

For good reasons, we have a culture of deliberation and care in the purchase of equipment and systems and supplies in our De-

partment of Defense, and we should. We want to be very careful to be sure that things work right. We want to be sure that we are doing things in an honest and proper way in the procurement process so that the process matches the requirements and budgeting needs of the Department of Defense. This culture which is understandably based upon due deliberation and process clashes with the hyperventilated culture of the tech world where, as Moore's Law would tell us, things always change in a big hurry, usually for the better.

So, when you combine the dynamic of the tech world with the more deliberative culture of Department of Defense procurement, you get some trouble. You get some challenges, and that is what we are here to talk about this morning.

I want to say from the very outset that the gap that has been identified between cost and value I do not ascribe to any weakness or deficiency by any individual or institution in the procurement process. I am not here this morning to say that someone has dropped the ball or has not done his or her job. I am sure that is true in some instances, but my sense here is that there is a systemic problem which owes itself to this culture clash that I mentioned a few minutes before, that it is a very hard thing to capture a whirling dervish, which is this technology dynamic, and tame it. It is a very difficult thing to do, and we do not want to go to either extreme, right?

We do not want an extreme where we say, buy the next thing that comes out, it will probably work. Well, that is really not a very good way to serve our uniformed personnel or our taxpayers.

On the other hand, we do not want to say we do not care how fast technology is moving. If something looked like it was the right thing to do in 2004, buy it in 2009 or 2010 or 2011 or 2012. We are looking for a happy medium between those two polarizing positions.

Now, the data would certainly show that we need that happy medium. Work by the Defense Science Board (DSB) task force, which dates back to November of 2000, tells us some very forboding statistics: Only 16 percent of all IT projects were completed on time and on budget; 31 percent of those projects were cancelled before completion; 53 percent were late and over budget with the typical cost growth exceeding the original budget by more than 89 percent, which is a very significant number; and of the IT projects that are completed, the final product typically contains only 61 percent of the original specified features. Now, that could be a good thing or bad thing.

I know one of the things that we are going to talk about this morning is how requirements creep, which in other areas of procurement is regarded as a bad thing, may well be a necessary and good thing in this field because of that technological dynamic that I talked about earlier.

At any rate, we have assembled a panel of three gentlemen who thoroughly know this subject, who, I think, will contribute much to our discussion this morning. We look forward to welcoming them.

At this time, I am going to turn to my friend, the ranking member from Texas, Mr. Conaway, for his comments.

[The prepared statement of Mr. Andrews can be found in the Appendix on page 29.]

STATEMENT OF HON. K. MICHAEL CONAWAY, A REPRESENTATIVE FROM TEXAS, RANKING MEMBER, PANEL ON DEFENSE ACQUISITION REFORM

Mr. CONAWAY. Well, thank you, Mr. Chairman.

I thank the panel for coming out this morning and for sharing your thoughts with us.

Today's hearing is going to focus on helping us understand how IT acquisition systems versus the normal, traditional hardware acquisition systems differ and how they should and getting a better understanding of the impact that different styles, for lack of a better phrase, go at this issue.

Clearly, information technology and the hardware attached to that is marketed differently. If you look at the F-4, which had about 8 percent of its systems run by computers, versus the F-22, of which like 80 percent of its systems are run by computer, it is a different world and growing.

The Vice Chief of Staff of the Army, Peter Chiarelli, has said that the antiquated system we operate is an albatross around the neck of the Army. The chairman has already mentioned the Defense Science Board's findings from the March 2009 report that says, in short, that the report found that the fundamental problem the Department of Defense faces is that the deliberate process through which weapons systems and information technology are acquired does not match the speed at which new IT capabilities are being introduced in today's information age. The report's principal recommendation is that the Department needs a new acquisition system for information technology.

While it is certainly easy to recognize that the introduction of new IT capabilities outpaces the speed of the acquisition system, what is less clear is what such a new acquisition system for IT would look like. Time will have to be a critical factor.

How will the Department minimize time of delivery while ensuring proper oversight and avoiding wasteful spending?

Another question is, is there a reason to believe that the DOD can be successful at such a new approach? If so, why wouldn't a similar approach work for traditional weapons systems?

This is particularly true as our weapons systems get more and more IT content. At some point, how does one distinguish between an automated information system, like a business system or Intranet, and an aircraft that has 80 percent of its functionality delivered from electronic sensors and information processing capability?

I look forward to hearing from our witnesses. I want to thank the chairman for starting this hearing right on time.

[The prepared statement of Mr. Conaway can be found in the Appendix on page 30.]

Mr. ANDREWS. Thank you very much, my friend.

I am going to, at this point, introduce our three witnesses.

Without objection, your opening statements will be included in the record of the hearing, and we would ask you to synopsize your written statements for us so we can proceed to questions.

I would also say that any member of the panel who wishes to have an opening statement entered, without objection, will be permitted to do so.

So I am going to read the biographies of the witnesses, and then we will proceed with synopses of your statements and then get on to questions and answers from the members of the panel.

Timothy J. Harp is the Deputy Assistant Secretary of Defense for C3ISR and IT Acquisition. Mr. Harp is responsible for the review of major acquisition programs for command, control, communications, intelligence, surveillance, reconnaissance, space and information technology programs. In addition, he leads reviews of major defense acquisition programs and major automated information systems as chairman of the command, control, communications, and intelligence overarching integrated product team in support of the Defense Acquisition Board and Information Technology Acquisition Board.

Mr. Harp received his bachelor's of science (BS) degree in business administration from Penn State University—he is a Nittany Lion—and a master's of business administration degree in financial management from the George Washington University. He is Defense Acquisition Workforce Integrity Act Level III certified in program management, business, cost-estimating and financial management and acquisition logistics. His awards include the Defense Meritorious Civilian Service Medal, the Defense Exceptional Civilian Service Medal, and the Defense Superior Service Medal.

Mr. Harp resides in Manassas, Virginia.

Welcome. Glad you are with us.

Mr. CONAWAY. Can you get that all on one business card—the command, control, communications, intelligence, surveillance, reconnaissance, space and information technology?

Mr. ANDREWS. We might have to introduce legislation that limits the name of any group to no more than three or four words. That would probably save us quite a bit of money in business card printing.

Dr. Paul Nielsen is director and chief executive officer of the Software Engineering Institute (SEI), a federally funded research and development center operated by Carnegie Mellon University. The SEI advances software engineering principles and practices through focused research and development, which is transitioned to the broad software engineering community.

The SEI serves as a global leader in process improvement and networked systems survivability. Additionally, the SEI is a key innovator in software architecture, software product lines, interoperability, the integration of software-intensive systems, and the increasing overlap of software and systems engineering.

In a very distinguished career in the United States Air Force, Dr. Nielsen served in the U.S. Air Force, retiring as a Major General after 32 years of distinguished service for which we thank him. In 2004, Dr. Nielsen became a fellow of the American Institute of Aeronautics and Astronautics (AIAA). He served as the AIAA president from 2007–2008. He serves on the Air Force Scientific Advisory Board and is a member of the board of directors for the Hertz Foundation, a nonprofit that awards graduate school fellowships in the applied sciences.

Thank you, Dr. Nielsen, for your service and for being with us this morning.

Finally, Dr. Ronald Kerber is an experienced executive with a successful record of leading and growing domestic and global businesses. His leadership responsibilities have included general management, innovation, product development, procurement, cost reduction, and profitability in diverse global organizations. He currently splits his time among a variety of entrepreneurial and pro bono activities as president of Small Business Development Center (SBDC), a small consulting firm; as partner and cofounder of Dominion Development Company and Profit Station, LLC; as visiting professor at the Darden Business School at the University of Virginia; and as a member of the Department of Defense Science Board.

Dr. Kerber received his BS degree from Purdue University and his master's of science (MS) and Ph.D. degrees in engineering science from the California Institute of Technology.

Gentlemen, thank you for your meticulous preparation. As I said, your written statements are considered to be part of the record.

Mr. Harp, we will begin with your oral testimony. We would ask you to summarize in about five minutes so we can get to questions from the panel.

Good morning.

STATEMENT OF TIMOTHY J. HARP, DEPUTY ASSISTANT SECRETARY OF DEFENSE, COMMAND, CONTROL, COMMUNICATIONS, INTELLIGENCE, SURVEILLANCE, RECONNAISSANCE AND INFORMATION TECHNOLOGY ACQUISITION, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DOD CHIEF INFORMATION OFFICER

Mr. HARP. Good morning Chairman Andrews, Representative Conaway and other members of the Defense Acquisition Reform Panel.

Thank you for this opportunity to testify on challenges to effective acquisition and management of information technology systems. I have submitted my written statement, as you mentioned, for the record, and will now briefly highlight a few key points.

Specifically, I would like to point out some challenges within the information technology environment that differentiate information technology acquisition from the major weapons systems acquisition that I experienced throughout my 22-year Navy career as a weapons system acquisition professional. I would like to contrast this to my recent experience over the past six years as a member of the IT culture that you mentioned.

Based on my experience, the traditional DOD acquisition process is far too slow to keep pace with the extremely rapid pace of information technology change. Even the different phases of the acquisition process, as set forth for weapons systems, are ill-suited for information technology systems. Phase A is intended to mature technology; yet our underlying information technologies are now largely matured in the commercial sector. Phase B is intended to ready a program for production; yet information technologies typically are not produced in quantity. Phase C is a production phase, which

again is generally not relevant to information technology that is not produced in quantity.

The term “life cycle” has also become ambiguous because, similar to the B-52 experience where we build an airframe and then update the pieces over time rather than build a full replacement, the inherent modularity and dynamics of information technology and the pace of commercial information technology development allow us to build or adopt the information technology equivalent of an airframe and continue to modify it indefinitely rather than replace an entire system in a predetermined period of time.

As noted by the recent DSB report, acquisition reform studies have been ongoing almost continuously since the original Goldwater-Nichols legislation was passed in 1986. Most often, acquisition-related problems in those reports have been attributed to requirements creep and funding instability.

With regard to information technology requirements creep, Moore’s Law, the hypothesis that the power of information technology will double every 18 months, has proven to be valid with regard to the information technologies that we acquire. This puts pressure on information technology acquirers to change the system-level requirements during the design process to enable the fielding of relevant technology.

In addition, combat operations are being conducted in rapidly changing circumstances, placing pressure to change requirements during information system acquisition to respond to adversary tactics. Also our customers, the warfighters of today, are information-technology savvy, often termed digital natives, with expectations to leverage the unprecedented innovation in the commercial market to enhance our information systems and capability in terms of agility, flexibility, responsiveness, and effectiveness, adding to the requirements creep pressure.

The combination of these three very real forces leads to significant requirements change pressure on our information technology process. We should begin to embrace the concept that changing requirements might actually be desirable for information technology acquisitions rather than to follow the inherent weapons system acquisition process assumption of stable requirements over time.

Funding stability in this dynamic environment is also a significant challenge to information technology acquisition. A large portion of the Department’s discretionary funding is allocated to acquisition. Within the acquisition accounts, information technology programs are relatively more flexible because, unlike weapons system programs, information technology programs typically do not have significant out-year production quantities to amplify near-term changes in the execution of budget year funding. So, when faced with a Hobson’s choice, the Department will defer to information technology more often than weapons system technology. This aspect of information technology programs tends to drive a degree of funding instability that adds to the requirements stability.

In short, the weapons system acquisition process is optimized to manage production risk and does not really fit information technology acquisition that does not lead to significant production quantities. Also, a foundational weapons system acquisition as-

sumption of requirements and funding stability is ill-suited for the information technology acquisition.

The information technology acquisition model proposed by the Defense Science Board recognizes the unique aspects of information technology, and addresses the requirements and funding challenges through the application of agile processes and exploitation of the inherent modular nature of the information technology to build smaller capability releases rather than large programs.

The Department welcomes the House Armed Services Committee (HASC) Fiscal Year 2010 defense language that gives the DOD the authority to establish 10 pilot programs to rapidly acquire information technology capabilities under an alternative acquisition process, and we look forward to working with this panel in the future to create an effective acquisition and management construct for the information technology systems. We also appreciate the committee's inclusion of section 1111, which would allow us to bring industry IT experts to DOD on an exchange basis to help with this effort.

Thank you.

[The prepared statement of Mr. Harp can be found in the Appendix on page 34.]

Mr. ANDREWS. Thank you very much, Mr. Harp. We appreciate that.

Dr. Nielsen, welcome to the committee.

STATEMENT OF DR. PAUL D. NIELSEN, DIRECTOR AND CHIEF EXECUTIVE OFFICER, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON

Dr. NIELSEN. Thank you, sir.

Chairman Andrews, Ranking Member Conaway, and other committee members, I thank you for this opportunity to appear before this panel, talking about a very important subject for our country.

There have been a number of excellent studies on defense acquisition over the years. They all pretty much agree on the findings and on the recommendations, and I know you are well aware of all of them. Rather than re-plow this sort of well-furrowed ground, I would like to talk about one aspect that, I think, is important and central to all of defense acquisition, and that is the whole side of software in defense systems. That is true in weapons systems, enterprise business systems, and IT systems.

Software is almost everywhere now, and the amount of software continues to grow, as was mentioned by Representative Conaway. Software engineering is a young discipline, and it is not rooted in the physical world like some of the other engineering disciplines such as civil engineering, aeronautical engineering, mechanical engineering, and electrical engineering.

Without physical constraints, the design space is so vast for these large programs, which need strong architectural principles, disciplined processes and talented people to be successful. The larger the program, the more important this is, and we know the Department has some of the larger programs.

The software engineering community has made major advances in the last 50 years, but the size, function and complexity of software has continued to grow. The bar keeps getting higher in these

areas. As mentioned, Moore's Law has helped us a lot by giving us more computational throughput, a lot of storage, but this has led to more and more functionality resting in software in all of our defense systems, and sometimes the line between what is an IT system and what is a major weapons system gets a little blurred now.

This is true not only in the defense world. This is true in the commercial world, aerospace, telecommunication, automotive, medical. Software is just everywhere. Cars now have almost 100 million lines of software in them. Telephones and cell phones that each of us has have 2 million to 10 million lines of software.

Tremendously innovative concepts keep opening up in the software engineering world and new challenges as well. We are now in an era when an increasing number of systems are linking via networks, such as the Internet. The convenience, power, and cost benefits of these approaches are compelling, but the complexity of architecting, developing, testing, and operating these ultra-large systems is daunting, and we are all becoming more and more aware of the pervasive cyber implications of these connective systems. We have to worry about that, too.

More than ever, we need strong quality built into our systems from the initial design and architecture. This is a major theme in software engineering over these last 20–30 years that, through strong architectures, disciplined processes and pervasive attention to quality, you can deliver complex systems on time and within budget. And yet, by following these principles, you will also develop software and IT systems that are more secure.

To accomplish this, we really need the entire community to understand software engineering principles and to work together to address the acquisition problems we face immediately and also to have some forward-looking research to address the problems that are coming down in the future. We will have even larger systems with even more connectivity.

IT systems have their own unique characteristics. We really have to worry about the different tempo that IT systems have and the ubiquity of IT systems, but we also need to worry about the systemic issues that affect IT and weapons systems programs as well.

As we look to the future, the bar is going to keep getting higher. There is no doubt about that. We are going to need government engineers and program managers who are trained and experienced to handle the systems we build, who understand the architectural principles and trades that are made and who have the expertise and passion for this business. We will need industry engineers and managers on the IT as well as on the weapons systems side who have kept up with the latest techniques and who have contributed to the best practices and innovations in software and systems engineering. We need robust research programs at our universities to address the opportunities and problems that are yet to come.

Mr. Chairman and committee members, with that, I will end my statement, and I look forward to your questions.

[The prepared statement of Dr. Nielsen can be found in the Appendix on page 48.]

Mr. ANDREWS. Dr. Nielsen, thank you very much. We appreciate your testimony.

Dr. Kerber, welcome.

STATEMENT OF DR. RONALD L. KERBER, CO-CHAIR, DEFENSE SCIENCE BOARD TASK FORCE ON DEPARTMENT OF DEFENSE POLICIES AND PROCEDURES FOR THE ACQUISITION OF INFORMATION TECHNOLOGY

Dr. KERBER. Thank you.

Mr. Chairman and members, it is a pleasure to appear before your panel. I am a member of the Defense Science Board, and I have submitted to you copies of three reports that inform my testimony.

Mr. ANDREWS. Without objection, they will be entered into the record.

[The information referred to can be found in the Appendix beginning on page 87.]

Dr. KERBER. Okay. I must also state that I am appearing as a private individual, and my comments do not necessarily reflect those of the views of the Department.

We have looked at the defense acquisition process, and as you well know, there have been many reports and many studies, and the question is: Why do these activities not address the problem that has lasted for so long? We would say that it does not address the root causes of the problem.

The problems appear to be caused by immature technology, requirements creep, funding instability, but we would argue most of that is caused by inexperienced and unproven leadership, and programs are not structured and initiated in a way that can be successfully completed. There is no silver bullet to solving this problem. It is really a commonsense approach.

We also think the problem is beyond the scope of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD-AT&L). It is really a problem of the scope of the Secretary of Defense (SECDEF), and it should be because many of those players who perform in the acquisition arena do not report to the Under Secretary of Acquisition.

So what is needed?

It seems simple, but we need to buy the right things. We need to select an effective leadership team. We need to reform and streamline the acquisition process, and we need to improve acquisition execution. We also need your support in helping the Department to do this, and we need to instill a sense of urgency.

Just a couple of comments on buying the right things: That seems simple, but we really need a resource-balanced business plan-type concept for the DOD that includes funded acquisition. We need to specify the capability needs to support our National Security Strategy. Then we need to also effectively represent the combatant commanders in the process of determining what we buy. Then we need to use comprehensive systems engineering and analysis early and throughout the process to determine what we are buying and how we are buying it. We need to avoid hard requirements without extensive analysis and trade-off.

Then we need to, secondly, select an effective leadership team. Acquisition cannot be fixed without a proven effective leadership team, and that goes back to the recommendation of the Packard Commission. Signs of poor leadership include poorly designed product development strategies, poor management of technical risk, the

selection of inexperienced contractors, poor contract incentives, and reward for change orders. Skills in program administration are often confused in the acquisition community with management ability. Managers manage what they understand. Proven experience should lead to better judgment and execution.

Another point that is equally important is that the Secretary of Defense has many offices that contribute to the decision process and acquisition, such as Program Analysis and Evaluation (PA&E), the Chief Information Officer (CIO), the Director of Defense Research and Engineering (DDR&E), the Comptroller, and the Operational Test and Evaluation (OT&E), plus the services, of course. Often these groups are not aligned. These groups must be aligned once a decision is made to have an acquisition or to buy something in the Department, and their constructive input should be early and continuous, not just at decision milestones.

We need to improve acquisition processes for major systems, commercial derivatives, information technology, and services. We need to establish more streamlined processes with in-depth analysis up front, planned spiral development and block upgrades, and the use of competitive prototypes.

For IT acquisition, these systems continue to grow both in size and in content in embedded systems. The DOD acquisition process is inconsistent with the rapid change of commercial IT technology.

You, Congress, have imposed new requirements to shorten the acquisition IT cycle time for all but national security systems. That is important, but the Department needs processes and the capability to do that.

We have recommended for the IT acquisition process a new streamlined decision process, and we have also recommended how and when to use it. We also want to point out that, as has been mentioned earlier, IT systems do not satisfy the laws of physics, and so we do not always know what we are buying, so we need to minimize the acquired system vulnerabilities. We need to adopt an IT acquisition strategy that confounds the enemy, using variety, change and rapid acquisition. The Joint Chiefs must assure that field commanders are trained to test information technology systems for authenticity and to operate them in degraded modes. We need to clarify IT off-site accountability. We need to strengthen the CIO authority for the enterprise to provide IT vision, policy and architecture, and we need to make sure that we identify clearly who has oversight accountability for all systems. As the growth of IT systems continues, that percentage of the total acquisition will grow, and we feel that that needs to be managed under the Office of the USD (AT&L).

We need to improve acquisition execution. I have talked about that in the report. I would just say a significant point is we need to right-size the acquisition workforce with experience. We can do that by process mapping the process and the workflow to determine the right size and to assure clear accountability and authority for everyone. Finally, we need to develop process metrics for all that we do.

Just one final comment. In the private sector, there are different characteristics for acquisition. The customer is clearly defined. The decision authority is more clear. Accountability is more clear. In-

centives are more clear. Yet it is very difficult to do this process even in the private sector, and few private companies really do it well. Especially for the DOD, it is very difficult to do this kind of process on a public stage.

Thank you.

[The prepared statement of Dr. Kerber can be found in the Appendix on page 62.]

Mr. ANDREWS. Well, thank you very much.

We appreciate the statements from each of the witnesses, and we will begin the questioning.

Mr. Harp, you made reference to the language that would authorize 10 pilot programs for an alternative acquisition process in IT, which the committee has supported.

Can you give us some thoughts about what principles you might rely on in that pilot process and what kinds of differences you would institute in the acquisition process?

Mr. HARP. Well, as we look to the inventory systems that we are considering, there seem to be four natural types of systems. We have some systems where we are buying just commercial, off-the-shelf hardware, and that is considered an IT system. That does not require the same process as a system where we are actually developing and writing software code and developing a capability by writing code.

Another type of acquisition that we do is we buy software that is commercial software, and we put it together, and we build the interfaces between the systems, so we develop a system of systems, if you will, using commercial off-the-shelf (COTS). So that would be a different approach as well.

So we are looking at some different templates on how we might approach that, but some of this becomes—I mentioned the B-52 model. If you get to a system where you do not really need to replace the core system—there have been studies that show, when you build a new system, up to 60 percent of the code you have to write to make it work does not get used over time, so we do not want to replicate building that 60 percent. A lot of times, we can take the core system that we have and just fix the piece that is broken or can add the capability that you need by building modules, right? With the funding discussion that I had, we have seen through our experience that many of these programs are level-funded over time, and the decision on how much you are going to fund in an acquisition program is actually made during execution rather than—

Mr. ANDREWS. But, in layperson's terms, what would you try to do differently in the pilot as opposed to what is being done now? How are you going to use the pilot to break new ground?

Mr. HARP. What I would do is take a larger system, identify the modules of that system and the interfaces, the commercial or standards that exist for those modules to talk together, and would approach each module as if it were a separate release, or a separate part of a system, rather than waiting for all the modules to be developed before we go to test. So you can test and release individual systems in an agile fashion, individual releases in an agile fashion, rather than waiting for the entire thing to be completed, because oftentimes we will have several modules under develop-

ment in parallel, and we cannot get to the final test until we complete the final module, and other modules that could be used are——

Mr. ANDREWS. I think it was your testimony that said that the average time to get to the finish line was about 81 months. Was that in your statement?

Mr. HARP. Yes, sir.

Mr. ANDREWS. What do you think a plausible goal is to reduce that to? In an optimal world, if the pilot worked great and became a great success, by how much time would we reduce that 81 months?

Mr. HARP. Well, conceivably, you could reduce it to 12 to 18 months, but again, you are not talking about delivering the same thing. The 81 months is a large system with several releases, with several modules, all delivering at the same time. In 12 to 18 months, you could deliver capability in pieces of that large system, so it is not really an apples-to-apples comparison.

Mr. ANDREWS. I assume this is where the open architecture and the standards become important.

Mr. HARP. Yes, sir. Yes, sir.

Mr. ANDREWS. If your first release in month 18 becomes obsolete by month 36, you have got to have a platform where it can easily be modified, an architecture where it can easily be modified, and not tear it up and start all over again. Am I right about that?

Mr. HARP. Yes, sir.

Mr. ANDREWS. Dr. Nielsen, one of the ideas that you talked about, and it really followed on Mr. Harp's testimony, was sort of changing the presumption of purchasing and procurement in the IT world. In the regular procurement world, although it is rarely met, the presumption is that the requirements you start out with should not change and that there has to be some burden of proof on he or she who wants to change the requirements. You are suggesting a different presumption, I think, in the IT purchasing world where you presume there are going to be changes because of Moore's Law, and you have a different question, but you also said that the line between software procurement and weapons systems is blurred.

Dr. NIELSEN. Yes.

Mr. ANDREWS. So how do we reconcile that problem?

If we were to take your idea and institutionalize in the law a different set of presumptions about requirements in the IT purchasing, where would we draw the line between the IT purchasing and the weapons system purchasing so we do not exempt weapons system purchasing from some very important adherence to requirements that we start out with?

Dr. NIELSEN. Well, sir, I think there are some things that are clearly pure IT systems, and I think Mr. Harp mentioned that. You know, if you look at the desktops of everybody in the Department of Defense, they have desktops that are commercially procured desktops for the most part—Dell, IBM, whoever—computers with Microsoft or Apple or whatever software. That is kind of clearly in the IT world.

Mr. ANDREWS. Right.

Dr. NIELSEN. But as you migrate more to command-and-control systems, which have an information technology kind of function,

you start to get to where life-and-death decisions are made based on these things, so it starts to migrate into the weapons system.

Mr. ANDREWS. I mean, is the data system in the cockpit of an airplane an IT acquisition, or is it a weapons system acquisition?

Dr. NIELSEN. You know, I would consider it a weapons system myself.

Mr. ANDREWS. Yes.

Dr. NIELSEN. But yet it certainly has some IT—

Mr. ANDREWS. You understand the importance of that question is not simply metaphysical.

Dr. NIELSEN. Yes, sir. Yes, sir.

Mr. ANDREWS. One of the driving forces in cost overruns and weapons systems is requirement changes.

Dr. NIELSEN. Right.

Mr. ANDREWS. Requirement creep.

If we want to wrestle that problem to the ground, we certainly want to keep the present presumption, which is that the requirements you start out with do not change.

On the other hand—and I hear what you are saying—if Moore's Law has pushed the envelope and, by year six of a procurement process, the system we are going to put in the cockpit is not the best one, we do not want to be stuck with that either.

Dr. NIELSEN. Yes, sir.

I remember, you know, I was the vice commander of the Aeronautical Systems Center, which buys the airplanes for the U.S. Air Force, from 1999 to 2000. At that point, even as the F-22 was coming into production, there were some parts that were no longer made for it that were baselined into the system because they were IT kinds of parts that were designed in the 1980s, and you know, in the year 2000, you are not going to have those parts anymore.

So we have a pace problem in all of our systems right now. I would like to see us experiment on the IT systems, especially with the ones that are more on the pure IT side; but if we find principles that work there—gosh knows we have some issues in the weapons system acquisition world, too—then maybe we can take those good ideas and best practices—

Mr. ANDREWS. This is what we are hoping, that Mr. Harp's pilot will lead us to some good data and to some good conclusions about that. My time is up for now.

I will turn to my friend Mr. Conaway for his questions.

Mr. CONAWAY. Thank you, Mr. Chairman.

Again, thanks, gentlemen, for being here.

You know, anecdotes drive a lot of stuff. I recall, in 2005–2006, the Army had a requirement for a biometric tool they could use in Iraq to capture fingerprints. There was an elaborate process of designing what that ought to look like, how much it ought to weigh, the battery. One of the deals was weight. They said it had to weigh seven pounds.

While they were trying to work that out, the commercial side of the world had a three- or four-pound thumbprint/fingerprint model that was available. You know, I do not know if it was at RadioShack, but it was available out there, so that kind of exemplifies the struggle that we have got.

Mr. Nielsen, you mentioned the laptops that everybody at the Pentagon is using and the struggle that most organizations have of making sure every three or four years those are, you know, redone or replaced or whatever. That is the mundane side of what we are talking about. Then you have got the clear message you mentioned about the F-22 in that, you know, it was 21 years between the start to the first time it landed at Langley to go to work.

Dr. NIELSEN. Yes, sir.

Mr. CONAWAY. There is a whole world of difference in the size and in the power of that deal.

The key, though, is people. Mr. Kerber, you mentioned that. At Price Waterhouse, if I could get the really bright staffers to work my jobs, my life was real easy. If I got the less—you know, the brand new rookies, my life was not very easy. So it all gets down to people. You know, your stereotypical IT person does not wear a uniform and does not work the same hours. I mean, it is a different culture altogether.

How do you get the right people who are willing to make those commitments? If you have got that background, how does the Defense Department keep them and incent them to stay on board? How do you address that?

Any of you.

Dr. NIELSEN. Perhaps I will answer a little bit on that.

When I was the commander of the Air Force Research Lab, we were always looking for great people, and we were competing with industry lots of times for the smartest people we could find. We found that there were lots of people who wanted to come work for the government. There are lots of people in our country who feel a commitment, and they want to provide some service for our country, whether it is in uniform or as civilians.

There are some impediments. One of the impediments we had that, I think, this committee is trying to address is, when we tried to hire people, it could take 9 to 12 months before we could bring them on board. Even if they were committed to us, if they were staring at an offer from a company that was ready to respond in two or three months, it was hard for them to wait for all that time.

Mr. CONAWAY. Is that because of security clearances or what?

Dr. NIELSEN. It is for all kinds of reasons, sir. It is not just security clearances. Some of it is just the personnel system itself. We have to be able to respond faster, and I think there are some innovative proposals that are being made for how we might respond faster to hire the kind of people who want to provide some service to our country.

Mr. CONAWAY. Mr. Kerber, any thoughts? You are out in the real world.

Dr. KERBER. I would think, first of all, the Department does offer very interesting and challenging problems, so that, by itself, is a little bit of a draw. Strong recognition would help. Also, you have several special programs to hire a specialist, if you will, and when we have looked at it, those programs have really been underutilized. You do also have a bonus structure that you can award bonuses for outstanding performance. So, between bonuses, recognition and giving challenging problems, you have an opportunity, if

managed right and effectively, plus the special hiring capability, to do that.

Mr. HARP. Today, the HASC section 821 is enhancing the expedited hiring authority for defense acquisition workforce personnel.

One of the things we could do to get these two cultures to cross the two cultures would be to expand that to include the IT workforce, including the Information Assurance (IA) personnel, who are trying to build up for our cybersecurity and that kind of thing. So, if we could expand that provision to include the IT workforce, that would be helpful to us. We have a parallel challenge in the IT culture that you mentioned in the acquisition culture. We need to bring them both along at the same time. So, if we could get that expanded to the IT workforce, that would be helpful.

Mr. CONAWAY. Yes.

Mr. HARP. I will mention, though, that I feel that there are some examples of where the weapons systems have successfully embraced the commercial technology. We have a submarine combat system that is based on commercial technology. The only hardware components in there that are not commercial are the transducers and the racks. The racks have to be special because they have to be water-cooled because of the fans, and air-cooled makes too much noise for the submarine. Other than that, all the cables, all the screens, all the circuit cards, everything in that system, and 80 percent of the software in that system is commercially procured.

The program has a lab-like environment, the program office that they have been running for almost 10 years now, that watches over the commercial industry and that follows the commercial industry. When one of those components is upgraded, they bring the piece in and test it and make sure that it does what it says it will do and that it has all the right requirements for our environment. When it gets a green light, then they plan on which submarine it will go in next, and they orchestrate that whole process.

So there are models out there that are like, as you mentioned, anecdotal, that show that we can make progress in this area. Now, there are some challenges with that model, and we are looking at that, but that is the kind of thing that we are trying to move towards to address this IT in the weapons system world.

Mr. CONAWAY. Thank you, Mr. Chairman.

Mr. ANDREWS. Thank you, Mr. Conaway.

The Chair recognizes Mr. Ellsworth for five minutes.

Mr. ELLSWORTH. Thank you, Mr. Chairman.

I benefit in the downside of being number three, as Mr. Conaway asked my first question about personnel and about finding that talent.

Mr. Kerber, I do not know when the last time was that you were in West Lafayette, but it is still alive and well.

Welcome to the Boilermaker.

Dr. KERBER. Good.

Mr. ELLSWORTH. Since we had the Nittany Lion comment earlier, I thought I had to throw one out there for Hoosiers.

Dr. KERBER. Thank you.

Mr. ELLSWORTH. We do that all the time, don't we?

Mr. ANDREWS. I understand. That is right.

Mr. ELLSWORTH. Dr. Kerber, could you talk a little bit more about—you made a comment about quick change to confound the enemy. I know, again, everything we are talking about is counter-intuitive to what we are saying of finding something that works and something that takes long to initiate. Then again, we want to change it because we know the enemy is constantly changing also.

I guess I just would like you to explore it a little more. I guess it goes back to Mr. Harp's module, which is that we get the base, and then we are plugging in new modules to change it. Is that kind of what we are talking about? Maybe you would like to elaborate more on that.

Dr. KERBER. Yes, let me just explain that in context.

First, we did one study where we said that the information management system of the Department needs to be considered part a weapons system because of the importance of it in managing combat and in managing our troops and their logistics, their availability, including precision weapons, et cetera. So, whether it is in the fighter aircraft or it is a handheld or it is a personal computer (PC), it should be managed as a weapons system and protected that way.

The issue you have when you change systems too rapidly, of course, is every time you change a software system, you need to take with that some training. And you can really have chaos in the field if you are not careful about how you manage training along with the introduction of new systems.

I would argue, whether it is in a fighter aircraft or in any other system, that you do need to plan for upgrades at the start of any program so that you can continually upgrade it in an orderly way. It does not have to absolutely track commercial technology, but it certainly does have to track it well enough so that you can keep current with replacement parts and the capability you would like.

With that, you would like to do things rapidly enough so that the enemy who is trying to penetrate your systems, especially some of the larger, sophisticated command-and-control systems, you would like to change parts of that so that their penetration of those systems is more difficult. So you have to balance the acquisition, the training and the confounding the enemy, if you will, as a group in order to have an effective weapons system.

Mr. ELLSWORTH. Dr. Nielsen.

Dr. NIELSEN. Yes, I would like to add just a little bit to that because he is right on in this regard.

One of the things, in the software engineering world, we talk about something called quality attributes. In the systems engineering world, they talk about nonfunctional requirements. One of the big quality attributes of nonfunctional requirements for all of our systems is actually the ability to evolve. I think that, when we see the IT systems, this may be one of the most important requirements that is out there; yet it is one that is often not specified. But we do not really start from scratch in any of these systems. We have systems that have to evolve over time, and I think if we start paying attention to more of that and architecting for the evolution of our systems, we would be in a lot better shape.

With respect to some diversity in our systems, we have, for the large part, what we now call a monoculture. A lot of our systems,

especially our IT systems, are Intel- and Windows-based. That means that if you are an enemy, if you are a cyber enemy, you know what you have to go against. It would be a lot better for us to have a little more of a diverse culture there and to have some systems that are not Windows-based and that are not Intel-based because that makes it harder for people to attack, and if they can bring something down, they cannot bring the whole system down.

Mr. ELLSWORTH. Thank you very much.

Mr. Chairman, we have got a tough road. I yield back.

Mr. ANDREWS. It is one we will traverse together.

The Chair recognizes Mr. Coffman.

Mr. COFFMAN. Thank you, Mr. Chairman.

There has been a movement afoot to say that we have outsourced too much in terms of the technical expertise engaged in the contracting process and that to improve the process, that we are going to bring a lot of that expertise back in and have them as Federal employees as opposed to private-sector individuals under contract. Some of you have addressed the issue about competing for expertise in the private sector versus the public sector.

Is that, in the world of the IT professional of needing to move this process along, bringing that expertise in-house versus having it available on a contractual basis as needed, is that movement going to hurt or help moving the IT process forward in defense acquisition?

Mr. HARP. Well, this argument is interesting in the IT world because, in the IT world, what we outsourced largely were people who were writing code, and what we are trying to bring in are software systems engineers who can manage contracts where the vendor is writing the code, but they understand the necessary hard points to make sure that it is done right and that it fits into the open environment we are trying to develop.

So we are not bringing back the same skill set that we outsourced, and we are bringing it back in a lesser quantity, and we will still be dependent upon industry to do the code writing and the things that are more dynamic while we maintain an ability to understand what we are asking for and an understanding of what they are delivering. So that is the balance we are trying to achieve, but we have a ways to go.

Dr. NIELSEN. Sir, I think you have really no alternative but to have people in the government who are educated at some level. They perhaps do not have to be the design engineers, but they have to have engineering awareness if they are making complex decisions. If they are managing programs that have engineering challenges in them, they have to know enough to know if what they are being told is right to make good decisions.

Another thing that is very important in this regard is that you cannot just rest on a person's education, you know, when they finish school in 1981 or in 1985 or whatever. This is an area that is expanding so fast that you have to have continuous education in this, so the government has to continue to send these people to short courses, long courses, whatever it is, to maintain their currency in this regard.

Dr. KERBER. Maybe I will make a couple of comments.

One is, I think you clearly need the leadership in the Department who understands the problem, who has actually done it well, and who can provide oversight and guidance and understand when things are in trouble and how to start and manage programs. So you certainly need that within the Department.

If you talk about, as was mentioned, creating code or creating even new ideas, I think you are really going to have to rely on the private sector for that because that is where that really comes in. I just think back to my many cases of managing technical people. If you have a large cadre of technical people in-house, they become very defensive of what they have designed and have developed. That is called the NIH problem, not invented here, and they are very resistant to ideas that come from outside. And so you need a capability to reach out, because if you do not reach out, you will never keep up with the private sector. So I would say there is a danger of having too much development inside that would actually thwart your ability to keep current on the outside.

Dr. NIELSEN. That is true.

Mr. COFFMAN. Thank you.

We have had testimony in prior meetings in defense acquisition whereby the issue about requirement changes would come up, and it might be that, you know, somebody just felt that they had a better way of doing it or that there was an analysis of current threat conditions and they had changed or something was left out, but that requirement changes were out of control, and that they were driving costs, and you know, that we needed to just kind of close the door at some point and say, this system is good enough. Let's just go forward.

On the IT side of that, is that just more straightforward in terms of the changing requirements for IT versus the hardware weapons acquisition process, itself?

Dr. KERBER. Maybe I will comment. A couple things.

One is I do know that our attention was brought to the Defense Logistics Agency (DLA) and them bringing in a new logistics system. The person in charge of that, I cannot remember his name. But anyway, he basically froze the requirements, brought in a system, and then opened it up for improvement. We would argue that the smart way to do that is at some point freeze requirements—I do not even like the word—freeze capabilities, introduce the system, make a list, then do a spiral development or block upgrade and have that planned from the get-go. Then you have an orderly way of bringing in new ideas. And you cannot continually just dribble them in. You have got to bring them in, in blocks, and maybe in the 12 or 18 month sequence, you bring in the new ideas you have. It is a very orderly way to do it. You can train your workforce. You can deliver the systems capability much quicker, and it is always essentially current.

Mr. HARP. Where that is a challenge is when you freeze the system for too long a period of time. You start running into Moore's Law. You start running into people that are saying, I cannot wait for this; I have got to do it now to get my job done, and they work around you. That is where some of that requirements churn comes in.

So I agree. You need to freeze it at some point, but you do not want to freeze it for a period of time so, when you deliver it, it is obsolete and you have got a huge cost to fix it and to implement it. So there is a balance there.

Again, it argues back to the DSB model that says, have shorter, smaller programs, and deliver things in modules rather than freezing an entire capability until you get the entire capability built, right? So, for each module, you might freeze that capability until you build it in the short period of time. That has more chance of success than freezing the entire capability until you deliver the entire system.

Mr. COFFMAN. Thank you, Mr. Chairman.

I yield back the balance of my time.

Mr. ANDREWS. Thank you very much.

Mr. Cooper is recognized.

Mr. COOPER. Thank you, Mr. Chairman.

I thank the witnesses.

I am worried that you IT guys basically are at the frontlines of a cyber war that is already happening, whether declared or undeclared. You get some attention but not that much. This is a war that is hard for people to comprehend because it is regardless of national boundaries or timetables or nationality or anything like that. So, with all the bureaucratic gobbledygook that we hear in these reports, there tends to be a certain lack of urgency and awareness. There also seems to be no more difference between capability and vulnerability because any system is attackable.

Dr. Nielsen mentioned, wouldn't it be nice to have diverse cultures? You know, we are so wedded to chips made primarily in mainland China that are so almost infinitely complex, that you add an infinitely complex software overlay of it with a couple hundred million lines of code, who knows? And are we hiring the best students from the best schools? You know, Mr. Conaway's question.

This is an area that should be focusing more national attention. So I am grateful for your all's expertise, but even in your testimony, I feel a certain lack of urgency. I appreciate Dr. Kerber's recent reports, excellent work for the Defense Science Board, but I have this nagging feeling that our defense establishment is not getting the best that the private sector has to offer and that we are having difficulty recruiting the best to join the government service.

I know there are a lot of wonderful people who have been patriotic enough to join and to survive the 9- to 12-month delay in hiring and all the bureaucratic rules, but I think we should be working as strenuously as possible to make it much easier for the best to come work for Uncle Sam and to stay working for Uncle Sam and to achieve things that leave Google and Microsoft and all these other high companies awestruck.

Yet I get the sense that we are more awestruck by them than they are by us. I know their compensation packages can be larger than we can imagine and things like that, but there has got to be a way so that we feel the urgency of this struggle because, when the Pentagon is hacked 35,000 times a day, when there is an allegation that someone has already stolen F-22 code, and various government departments were hacked just two or three days ago, you know, we are dangerously somnolent about this.

When I have talked to our defense friends and have asked them what kind of computers they have at home, it is never the system that is in the office. Never. I am not knowledgeable to know which one is better, but it is getting pretty scary here.

So I hope you gentlemen bring to your jobs a sense of urgency, and if these are truly SECDEF-level issues that are beyond, you know, under secretaries or assistant secretaries or anything like that, well, let's make sure the SECDEF is paying attention.

I think Gates, overall, is doing a great job, but for issues of this importance, it should not be, you know, a few sleepy folks at eight o'clock in the morning who are talking jargon that most people cannot understand. This is as important as Iraq or Afghanistan or anything because this is everything. This is every weapons system. This is the security of every American. This is the security of our banking system and tons of things so that these are no longer technical issues. These are life and death survival issues that, unfortunately, due to the science involved or the math or the technicalities, a lot of folks just are not getting.

So maybe to the extent you could help us translate these issues into plain, everyday English, it would be good because people have to enlarge their imaginations to be able to cope with the challenges they are facing. Right now, this is far more difficult for them to think of than biological warfare or things like that that are also exotic, but at least people have a sense of disease. They are less aware of viruses, computer viruses.

So this is more of a statement than a question, but I appreciate your all's expertise. Really, challenge this committee. Challenge your superiors to be the best that they can be.

That is all I have got, Mr. Chairman.

Mr. ANDREWS. I congratulate the gentleman for using the word somnolent, which is the first time it has been used in the committee's proceedings. I am very impressed by that.

Mr. COOPER. It is not a New Jersey word.

Mr. ANDREWS. No, it is not. You can't use a lot of New Jersey words here in this sort of place.

With the indulgence of my colleagues and the panel, we would like to offer people a second round of questioning. I am going to take that option myself.

The disturbing news is evident. And as I said at the outset, that 53 percent of the IT projects are late and over budget. Typical cost growth exceeds the target budget by 89 percent. This is at a time when our reliance upon software and IT work is growing in importance. An interesting chart, I believe it is from DSB task force. The F-4, 8 percent of its functions were performed by software in 1960. By 1970, the F-111 had 20 percent of its functions performed by software. By 1982, the F-16 had 45 percent of its functions performed by software. Then you get to 2000, the F-22, 80 percent. And I am sure that number is growing.

So the importance of this is growing, but the problem is worsening. I want to focus for a minute on the success stories. And I guess I would ask you which entities, if any, within the DOD world have different results? Which entities have proven to be successful models at the acquisition of IT products? Are there some corners of our system right now that are working well or at least better

than these data? If so, who are they? Where are they? And what have they gotten right that the rest of the system hasn't?

Dr. KERBER. I will just comment, Mr. Harp mentioned the submarine program, which is designed to be changed out with COT systems in an orderly way. And as we looked at it, it was one of the top managed programs in IT in the Department.

Mr. ANDREWS. Now, Dr. Kerber, to what do you ascribe the relative success of that program? I think I know, but I would like to hear you answer the question.

Dr. KERBER. Well, they do have strong leaders, and the leaders come up through a program in the Navy that is—trains them basically. But also they have designed the whole system and process around the concept that they need to refresh it periodically. And so they can do that in an orderly way by the way they set the capabilities that they need, how they acquire them, et cetera. So the whole program is structured for success basically.

Mr. ANDREWS. Do you know offhand the data that would compare, the data I just used about how they matched up with respect to time and budget in the submarine program?

Dr. KERBER. I don't, but I know they were doing a good job. I don't know the numbers.

Mr. ANDREWS. I think what we will do is ask the staff to just supplement the record. That was kind of a pop quiz. I wouldn't expect you to know it.

Dr. KERBER. I don't work for the Department incidentally.

Mr. ANDREWS. One of the things we want to do in this panel is to look at problem areas without question, but also look at some success areas and try to learn from those best practices.

One of the statements, I am not sure which, said it is very important not to use problems as a stick to beat people over the head with. I am not sure whose testimony that was in, but I appreciate that. I said at the outset, I don't think we have a lot of incompetent, ill-intentioned people creating these problems. I think the opposite is true. We have a lot of really dedicated, competent people who are working within a system that is just not serving them very well. So we want to find the instances where there has been success and learn from those instances and try to replicate them.

Would either of the other two witnesses want to answer that question.

Mr. HARP. We have had some success. We are kind of in what I call an interim ugly period right now. Because we are going from these large systems that evolved using proprietary software, millions of lines of code; we are trying to evolve to a system that is more of a layered process, as service oriented architecture (SOA) or cloud computing or some of these new concepts. And as we progress into those new realms, it gives us much more ability to control the dynamics of the IT world. Where if you are in a proprietary environment, it is very difficult to do that.

One of the agencies that is out in front in that area right now that is making some progress is the National Security Agency (NSA). They have a couple of programs that are not—I don't want to say they are—I don't want to hold them up as saying complete, but they are making progress in the right direction here. And they are a little bit out in front on that. So I would hold them up as

a good example. They turned around their process in the last few years and have made some good strides.

Mr. ANDREWS. Dr. Nielsen, do you have any—

Dr. NIELSEN. Sure. Sure. This is an area that teaches a lot of people humility, and as Churchill once said, we have a lot to be humble about in this business.

Mr. ANDREWS. We in the Congress fully understand that.

Dr. NIELSEN. But there are some success stories out there. They are too isolated. Naval Air Systems Command (NAVAIR) has done some wonderful work, especially on reengineering software on some of the maintenance software that they build for systems that are already in existence.

Warner Robins in the Air Force has done a really wonderful job on elevating their software game and doing pretty well on some of the software that they provide.

The Army has had a really interesting story over the last five or six years where they have crafted an education program for all their senior leaders, acquisition leaders, to be more aware of software engineering principles, architecture and such. And we are seeing some effect of that as it—

Mr. ANDREWS. Is that done through the War College?

Dr. NIELSEN. It is done some through DAU, the Defense Acquisition University, and some through an Army-specific program. And the people at Army Redstone in Huntsville have particularly benefited from that.

Mr. ANDREWS. I know Chairman Skelton has an acute interest in military education. He will be interested in that.

Dr. NIELSEN. And then there are some in the intel community, too, that is a little harder to talk about. But there have been some successes in the intel community as well.

Mr. ANDREWS. Very good. We are going to look more closely at those examples, because, again, we want to identify places where people are making progress and try to replicate those models.

Mr. CONAWAY, did you have follow-up questions?

Mr. CONAWAY. One other question, real quick question, is in line with the successes. But does DOD have an enterprise-wide set of metrics that says, here is what success would look like in the IT world? And then, do they actually systematically and comprehensively collect data over time to measure various systems against those metrics to say—in fact, flush out who the good guys—who are having successes and who have been humbled is a better way to put it?

Mr. HARP. The metrics that we have been using have been the financial metrics and the acquisition process metrics. And the whole purpose of this study in committee is that we found they don't work very well in measuring IT success. Because of the churn in the technology, if you say I want to have an acquisition baseline and, five years later, I am going to deliver something, five years later you can deliver something that the warfighter thinks is great but is totally broken from an acquisition perspective because it was successful.

We have built systems for a small group, and it worked so well in other groups that say, hey, I want that, too. And pretty soon the system that was intended for 10 people is now being used by 1,000,

right? So the cost went up tenfold, and it generates a statistic like we are mentioning here that you add cost growth, but in fact, it was a successful system because it expanded beyond what they imagined it would do.

So I don't think we have a good set of metrics, and that is part of what we are trying to develop here as part of this effort. And I guess I will just leave it at that. I think that the financial metrics and I think the milestone metrics for a fixed big program are the wrong metrics. I know we have been successful—you will see a correlation between the successful programs that we find and mention and size. Smaller programs are more successful. If we are delivering—we can compete with industry delivering programs of 75,000 lines of code or less. When you start getting up into the million lines of code, even industry can't deliver them on time and schedule. And so that kind of suggests that this whole direction that we are going with the small modular approach may lend itself to more successes.

Mr. CONAWAY. Anybody else?

Dr. NIELSEN. Yes, sir.

Sir, I am a strong proponent of earned value management. The DOD uses that, but sometimes not to the level of fidelity that they need early in a program. We found that if you do this where you really get credit—you plan what your work is going to be, you budget what your work is going to be and then you measure against how that is being done, you have to do that at a fine enough level of detail to get an early indication of whether you are successful. It is not good enough to find out five years into a program, because then you are really in trouble. We have had some successes with that in the military.

The Navy program has done that somewhat. NAVAIR has done that. But in addition, we have worked with some of the commercial companies and had great success with this. The one we are most proud of I think is some of the work we have done with Intuit, that of course works on Turbo Tax and Quicken and some of those products that follow some of these principles and has seen a remarkable improvement in their productivity and in their ability to meet their schedules, which obviously for tax software was very important.

Mr. CONAWAY. Thank you, Mr. Chairman.

Mr. ANDREWS. Mr. Ellsworth, any follow-up? I am sure you are going to say that the good example is these Boilermakers.

Mr. ELLSWORTH. I was just going to say that, now that Mr. Cooper is gone, I think what he was really trying to say, and being from Tennessee he will understand, that everybody wants to shoot the rabbit, but nobody wants to skin it, is an old saying. And that makes it much more simple for me being from Indiana.

I guess my question then is, who do we need to skin the rabbit? Like you said, is it the SECDEF? Is it you, Mr. Harp? Is it us? Is it all of us together? Are we moving in the right direction? I keep hearing we need to, we need to, we need to. And like Dr. Kerber said, all the studies—who needs to be skinning the rabbit, and how do we implement that? Let's move forward. That is what this panel is convened to do, is kick this ball down the court in the right direction. So help us implement what we need to be doing.

Dr. NIELSEN. I think it is a combined responsibility. And the DSB is right on about the importance at the very senior leadership levels how important this is. And even that at some points the Under Secretary of Defense for Acquisition, Technology, and Logistics isn't high enough; that it requires everybody to be in this.

But I also believe that a lot of acquisition is done at the contact point. And so you need smart program managers, smart system engineers kind of working on this as well. I mentioned in my statement, this requires the whole community to do this. And everybody has to feel responsible.

Mr. ELLSWORTH. If there are specific things that you all see about that, the hiring of folks—and I know that taking the nine months versus three, whatever it is that you can see to put a bug in our ear of people we can get to, we would be glad to take that on and try to speed that up to do exactly these things you are saying that we need to do.

Thank you, Mr. Chairman. I would yield back.

Mr. ANDREWS. Thank you.

Mr. Coffman, any follow-up.

Mr. COFFMAN. No, Mr. Chairman.

Mr. ANDREWS. Well, I would like to thank the witnesses, as I said, for a very thorough, well thought-out testimony this morning. We are going to be calling upon you again as the committee proceeds. Our intention is to explore these areas for the balance of 2009 and then convene early in 2010 and identify the best practices and recommendations that we will make in the form of legislative recommendations for the fiscal year 2011 authorization bill. So that is the timetable we are on.

I think this morning was both confirmatory, and it opened up some new areas of inquiry for us that certainly confirm, Dr. Kerber, our sense that the quality of the people, the human leadership is the pivotal point. I just think that can't be said enough.

Dr. Nielsen, I think that you identified and confirmed a point that we understand, that the acquisition process for IT is just very different than it is for lots of other things, and we can't superimpose that same orthodox model.

And then, Mr. Harp, the reason the committee supported the language for these pilots is we want you to be innovative and creative, and we are encouraged that you are going to do that.

What I found interesting and somewhat groundbreaking this morning was some of the testimony about the successes that we have had. We do want to learn more about that because we think that there can be successes that need to be highlighted and learned from so that we can find the best practices that these better leaders are implementing and replicating it and do more of it.

Again, we would welcome comments from the witnesses as we proceed in this process. It is our goal not to write a whole bunch of new rules, but to produce some legislative recommendations that would help fix this problem.

And I would like to thank our colleagues for their time and attention this morning and invite the witnesses to continue to correspond with the panel.

And with that, I declare the hearing adjourned.

[Whereupon, at 9:12 a.m., the panel was adjourned.]

A P P E N D I X

JULY 9, 2009

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JULY 9, 2009

Chairman Andrews
Statement for the Record
Thursday, July 9, 2009
Challenges to Effective Acquisition and Management of Information Technology Systems

Welcome to today's hearing on Challenges to Effective Acquisition and Management of Information Technology Systems. The panel has held a number of hearings to date to explore how we measure the performance of the acquisition system in meeting two critical goals: 1) rapidly filling warfighter needs; and 2) protecting taxpayers.

"Today we move on to the next question on our work plan: what are the root causes of failure in the acquisition system, particularly as they relate to information technology (IT) systems? We start today with the hypothesis that IT systems are qualitatively different from traditional hardware-oriented acquisition programs, and yet the Defense Department tries to force these IT programs into an ill-suited acquisition process that takes 5-15 years to develop and deploy a weapon system.

"For IT systems that increase functionality on 18 month cycles, that acquisition system fails the warfighter miserably. There are some statistics related to the performance of IT programs within this process that are telling:

- Only 16 percent of all IT projects complete on time and on budget.
- 31 percent are cancelled before completion.
- The remaining 53 percent are late and over budget, with the typical cost growth exceeding the original budget more than 89 percent.
- Of the IT projects that are completed, the final product contains only 61 percent of the originally specified features.

"That data seems to indicate that there are some significant issues with how the Defense Department acquires and manages IT programs that I believe deserve special attention.

"We have with us the Mr. Tim Harp, the current Deputy Assistant Secretary of Defense for Command, Control, Computers, Intelligence, Surveillance and Reconnaissance & Information Technology Acquisition; the Director and Chief Executive Officer of the Software Engineering Institute, Dr. Paul Nielsen; and Dr. Ronald Kerber, who recently served as the Co-Chair of the congressionally-mandated Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology. Gentlemen, we appreciate the fact that you are here today to share your expertise in acquisition with us.

"Let me now turn to our panel's ranking member, Mr. Conaway of Texas, for his opening remarks."

Statement of Rep. Conaway
Hearing of the
Defense Acquisition Reform Panel
on
“Challenges to Effective Acquisition and Management of
Information Technology Systems”
July 9, 2009

Good morning, Mr. Chairman, ladies and gentlemen. I would like to thank our witnesses for taking time out of their busy schedules to be with us this morning.

As the Chairman said, the focus of today's hearing is to get an understanding in regards to how the acquisition process differs for information technology (IT) programs vice traditional, hardware-oriented acquisition programs. There is no doubt that the information revolution has had a profound impact on how we as a nation do business, which has also had a significant effect on how we provide for the common defense. Twenty years ago, every once in a while you

might see someone at the airport talking on a device the size of a shoe called a cell phone. Today, kids in elementary school have cell phones smaller than their hands (which also plays music and videos). In the 1960's the F-4 Phantom aircraft had approximately eight percent of its functions performed using software. Today, the F-22 has approximately eighty percent of its functions performed using software.

The question is whether IT programs should follow the same acquisition process that traditional hardware weapon systems follow. Speaking at an IT related conference on June 25, 2009, General Chiarelli, the Army Vice Chief of Staff of the Army, stated that "The antiquated system we operate under has become the albatross around the Army's neck."

As the chairman knows, in 2008 Congress requested that the Defense Science Board conduct a review of defense policies and procedures for the acquisition of information technology. That report

was recently completed in March 2009. I know our witnesses are very familiar with this report and its findings. In short, the report found that ‘...the fundamental problem the Department of Defense (DoD) faces is that the deliberate process through which weapon systems and information technology are acquired does not match the speed at which new IT capabilities are being introduced in today’s information age.’ The report’s principal recommendation is that the Department needs a new acquisition system for information technology.

While it’s certainly easy to recognize that the introduction of new IT capabilities outpaces the speed of the acquisition system, what is less clear is what such a “new” acquisition system for information technology would look like. Time would have to be a critical factor, but how would the Department minimize time to delivery while ensuring proper oversight and avoiding wasteful spending? Is there reason to believe that DoD can be successful at such a new approach – and, if so, why wouldn’t a similar approach work for traditional weapon systems?

This is particularly true as our weapon systems get more and more IT content. At some point, how does one distinguish between an automated information system, like a business system or an intranet, and an aircraft that has 80% of its functionality derived from electronic sensors and information processing capability?

I look forward to hearing from our witnesses and gaining their insights into this critical issue.

Thank you Mr. Chairman.

RECORD VERSION

STATEMENT BY

MR. TIMOTHY J. HARP

**DEPUTY ASSISTANT SECRETARY OF DEFENSE,
FOR COMMAND, CONTROL, AND COMMUNICATIONS,
INTELLIGENCE, SURVEILLANCE, RECONASSIANCE
AND INFORMATION TECHNOLOGY ACQUISITION**

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

DEFENSE ACQUISITION REFORM PANEL

OF THE

**COMMITTEE ON ARMED SERVICES ON "CHALLENGES TO
EFFECTIVE ACQUISITION AND MANAGEMENT OF INFORMATION
TECHNOLOGY SYSTEMS"**

JULY 9, 2009

**NOT FOR PUBLICATION
UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES**

Introduction

Good morning and thank you for this opportunity to testify before the Defense Acquisition Reform Panel of the Committee on Armed Services on “Challenges to Effective Acquisition and Management of Information Technology Systems”.

I am the Deputy Assistant Secretary of Defense for Command, Control, Communications, Intelligence, Surveillance, Reconnaissance and Information Technology Acquisition (C3ISR & IT Acquisition) within the Office of the Assistant Secretary of Defense for Networks and Information Integration. In my position within the Department of Defense (DoD), I am responsible for overseeing assigned major defense acquisition programs and major automated information systems by serving as an advisor to the milestone decision authority (MDA) for these programs. As an advisor to the MDA, I support decision-making on whether an acquisition program should be initiated and whether that program should proceed into the various phases of the acquisition life cycle. At each major decision point, the MDA must determine whether the program or a key increment of the program should be terminated, modified or approved to proceed. One key component of this responsibility is determining whether the program is complying with the Department’s acquisition policies documented in the DoD 5000 series and the requirements of the subtitle III of U.S.C. title 40 (formerly called the Clinger-Cohen Act). The other key component of my responsibility is to leverage my experience in determining the likelihood that the ongoing acquisition program will offer value to the warfighter within its approved acquisition program baseline.

Additionally, I participate in forums and support activities to improve the acquisition process; examples of this range from sanctioning lean six sigma studies within my office to partnering with trade associations in studies pertaining to industry trends with our industry counterparts or offering testimony to various groups such as the recent Congressionally-directed Defense Science Board (DSB) on the Policies and Procedures for Acquisition of Information Technology or the ongoing National Academies Committee on Improving Processes and Policies for the Acquisition and Test of Information Technology in the DoD. I realize that improvement is essential and have great respect for those efforts that continue to strive to bring unity to our efforts as we work to improve the DoD acquisition process. In this regard, I agree with and support many of the recommendations from the recent DSB on the Policies and Procedures for Acquisition of Information Technology.

I would like to share my thoughts on a few key topics; specifically, challenges within the information technology acquisition environment, addressing requirements and funding instability, creating an effective governance construct and strengthening the industrial base.

Challenges Within Information Technology Acquisitions

As noted by the recent DSB, acquisition reform studies have been on-going almost continuously since the original Goldwater-Nichols legislation was passed in 1986.

Very often, acquisition-related problems are attributed to inadequate requirements definition and program funding instability. The question then arises as to whether these challenges are common to all acquisitions including those associated with modernizing and supporting the Department's ability to field information technology in a timely and cost-effective manner.

Based upon my experience, requirements creep and funding instability are challenges that will always be present and ought to be recognized as "fact of life" within the lifecycle of an information technology acquisition program. The time from first funding to initial operational capability has averaged 81 months for information technology systems. This is a relatively lengthy period of time during which there are significant pressures for both requirements and funding changes.

With regard to requirements creep, Moore's Law, the hypothesis that the power of information technology will double every eighteen months, has proven to be valid with regard to the information technologies we acquire. This adds a dynamic factor to information technology system acquisition that puts pressure on system builders to change system level requirements during the design process. Also, combat operations are being conducted in rapidly changing circumstances, shifting from humanitarian operations to intense combat operations with little or no warning, that involve our multinational and interagency partners. This drives capability type requirements changes for systems to be used on the edge.

Likewise, our customers, the warfighters of today, are information technology savvy, often termed “digital natives,” with expectations to leverage the unprecedented innovation in the commercial market to enhance our information systems capability in terms of agility, flexibility, responsiveness and effectiveness, also driving system design requirements change. The combination of these three very real forces leads to significant “requirements change” pressure on the acquisition process. This observation was reflected in the 2006 Defense Science Board Summer Study on Information Management for Net Centric Operations where it was cited that information management in Iraq and Afghanistan was a principal concern among war fighters. In the 2006 DSB study, it was also noted that significant ad hoc activity was taking place, especially at the tactical level, to gain desired capability. Especially important was that much of the military capability used to support the conflicts was paid with supplemental funding—programs that were not part of the Department’s planned capability. Therefore, it should be no surprise that given Moore’s law and the persistent demand from our digital native customers, “requirements stability” within this environment is a difficult challenge and we must begin to embrace the concept that changing requirements might actually be desirable for information technology acquisitions. Akin to the lack of requirements stability, funding stability in this dynamic environment is a significant challenge that must be addressed within the existing acquisition governance framework.

A large portion of the Department's discretionary funding is allocated to acquisition. Within the acquisition accounts, information technology programs are relatively more flexible because, unlike weapons system programs, information technology programs typically do not have a significant out year production quantity to amplify near term changes in the execution or budget year funding. In terms of program funding, the inherent flexibility of information technology systems is like a double-edged sword. When a source of funding is needed, information technology programs are more likely to be used as that source. Also, when a rapid capability improvement is necessary, information technology is more likely to be a recipient of funding as noted previously.

In summary, both requirements and funding for information technology have been and will continue to be under pressure for change over time due to factors independent of the acquisition process.

Addressing Requirements and Funding Instability

As noted earlier, the DoD has the opportunity to leverage the unprecedented innovation driven by commercial market to enhance our weapon system's capability. Nevertheless, achieving such results involve significant change to processes, practices and commonly held beliefs institutionalized across the community. One such change is to move away from the large, "toll gate" decision acquisition program model to a model that encourages smaller acquisitions, both

in content and complexity. This observation was embodied in the March 2009 DSB report, "Policies and Procedures for Acquisition of Information Technology," by the proposed acquisition model that contained a single milestone with multiple "knowledge points" interspersed throughout the acquisition lifecycle. The proposed DSB model recognizes the unique aspects of information technology and provides more value-added activities including enhanced stakeholder engagement and analytical rigor throughout the acquisition life cycle. Developing tomorrow's net-centric systems will likewise require an approach to acquisition where the large waterfall model (with its long requirements, analysis, development and test phases) ought to be replaced with an iterative model that embraces requirements prioritization as well as multiple development/operational tests to support the delivery of mission capability throughout the system lifecycle. Even the different phases of the acquisition process as defined for weapons systems are ill-suited for information technology systems. Phase A is intended to mature technology, yet the underlying information technologies are now matured in the commercial sector, independent of DoD. Phase B is intended to ready a program for production, yet information technologies typically aren't produced in quantity, they are deployed as a unit of one. Phase C is the production phase, which again is largely not relevant to information technology. In fact, even the term "lifecycle" has become ambiguous because if designed well, it may be in our interest to move to a never-ending program concept for information technology acquisition. Similar to the B-52 experience where we built an airframe and then

updated the pieces over time rather than build a like replacement in its entirety, the inherent modularity of IT, the dynamics of IT technology, and the pace of commercial information technology development allows us to “build or adopt an airframe” based on an open design with commercial standards and continue to modify it rather than replace it in its entirety after a pre-determined period of time.

The fundamental concept of large information technology programs with distinct “beginnings” and “ends” is in question as we learn more about the inherent modularity of information technology and become more dependent upon commercial hardware that is evolving due to factors out of the control of the program manager. As we take advantage of the commercial market and move to more open designs that lend themselves to reuse and modification, we will find more value in modification of parts of the system rather than starting over with a clean sheet of paper for a total system replacement.

This approach is often referred to as a service oriented architecture (SOA) and presents a different set of challenges than the classical systems acquisition process. Recently, my office partnered with the Association For Enterprise Integration (AFEI) to develop a white paper designed to help government Program Managers better acquire service oriented architecture (SOA)-based information technology solutions. This study group, which was composed of experts across the DoD

industry base, concluded that speed by which DoD moves toward service-orientation is dependent upon such acquisition models like that recommended in the 2009 DSB study and the willingness of the leadership to allow such change.

I welcome the recent House Armed Services Committee fiscal year 2010 defense language that authorizes the DoD to establish ten pilot programs to rapidly acquire information technology capabilities under an alternative acquisition process. In support of this, I have my staff developing more detailed guidance/instructions that offers the next level of detail to the proposed DSB model contained in the March 2009 DSB Report on the Policies and Procedures for Acquisition of Information Technology.

Creating an Effective Governance Construct

Governance in this context relates to decisions that define expectations, grant power, or verify performance that is embodied by the structure and relationships among key stakeholders. As noted by the recent DSB report, significant change is required not only within the acquisition framework but also extends to requirements and test governance constructs. It was cited that the current governance model is characterized by rigid processes, long phases separated by infrequent decision gates and extensive planning documentation. This compares to the commercial information technology marketplace that embodies speed, agility, domain expertise and user-centered focus. It should be noted that we have

made strides forward. For example, the Joint Staff has introduced a new requirements validation process for information technology programs via the concept of the “IT Requirements Box.” This construct should reduce the requirements validation by pushing-down subsequent requirements validation to lower levels provided the program remains within established program criteria.

Additionally, the concept of community of interest (COI) has been successfully being implemented on the Distributed Common Ground/Surface Systems (DCGS) that offers an alternative approach to the existing governance approach. The DCGS COI concept addresses the two key imperatives needed in an effective governance structure by defining the boundaries of the organizational structure and relationships of the stakeholders. By shifting focus from capabilities and services resident within a single program of record to shared services across the DCGS Family of Systems, the motivations of individuals and organizations are aligned to a specific mission area (e.g., HUMINT, SIGINT, etc). Likewise, these communities are partitioned into a common grouping of core functionality composed of common infrastructure, enterprise services and mission applications focused to address those common issues while creating “enterprise behavior” rather than traditional program-centric or Service-centric behaviors.

We need to leverage such successes and implement a more effective governance system that can be replicated across the Department and is more applicable to rapid pace of information technology modernization efforts.

Strengthening the Industrial Base

Unlike typical hardware acquisition, Information Technology is perhaps the most inherently modular capability that exists within the DoD and therefore remains viable for competition throughout its life cycle. However, this has often been stifled since past information technology programs have followed the hardware-centric paradigm of gathering requirements to create a single large acquisition program and solicitation. This model incentivizes design of unique, proprietary systems that precludes taking full advantage of commercial technology and keeping pace with the dynamics of the IT industry.

Given Moore's law, the technology changes faster than the requirements process, faster than the budget process, and faster than the acquisition milestone decision process. As a result, by the time the acquisition program baseline is established, the technology being acquired is often out of date. In order to meet reasonable demands of our digital native customers and best use precious taxpayer resources, we often need to update programs soon after they have been baselined, and should change them several times between the milestones as defined within the existing

process. Much of the mandatory documentation supporting is overly prescriptive and also quickly becomes obsolete and inapplicable.

Our study results correlate well with the 2009 DSB study supporting enhanced competition through multiple firm-fixed priced contracts for small segments of the program that can be executed rapidly. Also, employment of standards-based reference models and well-defined and published commercial interface standards in lieu of unique DoD standards would improve time to market, competitive posture, and cost.

Creation of a standards-based open system would serve to mitigate the specification of a system for a company's product and also help prevent restrictive Intellectual Property and vendor lock-in. One of the main program office tasks would be to ensure the openness of the system to minimize unfair competitive advantage and "proprietary lock-in." As an example of this construct, my office has again partnered with AFEI and the Under Secretary of Defense for Intelligence to create an industry advisory group in support of the DCGS family of system governance construct. I look forward to the results of this effort that will investigate various business models to improve our ability to strengthen the industrial base.

Conclusion

The 2006 Quadrennial Defense Review Report highlighted the issue, noting, “as we emphasize agility, flexibility, responsiveness, and effectiveness in the operational forces, so too must the Department’s organizations, processes and practices embody these characteristics if they are to support the joint warfighter and the Commander in Chief.” Today, we have an opportunity to leverage excellent work completed by the Defense Science Board to improve the acquisition of the model for the DoD to effectively adapt modern information technology practices that may result in unprecedented relevance and value in support of current wartime operations. It will require significant change to address the underlying cultures that are embodied in existing processes, however a move to more B-52 type programs with smaller, shorter duration modifications rather than large systems acquisitions will lead to delivery of more relevant technology to our digital native warfighters at lower costs to the taxpayers.

I welcome House Armed Services Committee fiscal year 2010 defense language that gives DoD the authority to establish ten pilot programs to rapidly acquire information technology capabilities under an alternative acquisition process and look forward to working with this panel in the future to create an effective acquisition and management construct for information technology systems.

Thank you.



Timothy J. Harp

Deputy Assistant Secretary of Defense, Command, Control, Communications, Intelligence, Surveillance, Reconnaissance & IT Acquisition

Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (OASD(NII)/DoD CIO)

As the Deputy Assistant Secretary of Defense for C3ISR & IT Acquisition, Mr. Harp is responsible for the review of major acquisition programs for command, control, communications, intelligence, surveillance, reconnaissance, space and information technology programs. In addition, he leads reviews of major defense acquisition programs and major automated information systems as the Chairman of the Command, Control, Communications, & Intelligence Overarching Integrated Product Team (OIPT) in support of the Defense Acquisition Board (DAB) and Information Technology Acquisition Board (ITAB). He also supports the Under Secretary of Defense for Intelligence by reviewing the acquisition programs under development by the defense intelligence agencies.

Mr. Harp's previous assignments include service as the Director, Acquisition for C3ISR & IT Acquisition, the Program Executive Officer and Transition Lead for Financial Visibility, Business Transformation Agency (BTA), the Component Acquisition Executive and Head of Contracting Activity for the Defense Finance and Accounting Service (DFAS), and Assistant Deputy Under Secretary of Defense for Innovation and Technology Integration.

Prior to his promotion to the SES level, Mr. Harp served in the Immediate Office of the Under Secretary of Defense for Acquisition, Technology and Logistics as a Special Assistant to the Under Secretary. A retired Navy officer, he served for over 20 years in acquisition, logistics and financial positions at all echelons of the Navy and the Department of Defense. He also served afloat aboard the cruisers USS Leahy (CG-16) and the USS Ticonderoga (CG-47) where he participated in several deployments and exercises, including the Operation El Dorado Canyon Libyan strikes.

Mr. Harp is currently a government co-chair to the American Council of Technology/Industry Advisory Council, Acquisition Special Interest Group. He is a founding member of the White House Military Aides Association and a member of the American Society of Military Comptrollers.

Mr. Harp received a Bachelor's of Science Degree in Business Administration from Pennsylvania State University and a Master's of Business Administration Degree in Financial Management from the George Washington University. He is Defense Acquisition Workforce Integrity Act Level III certified in Program Management, Business, Cost Estimating and Financial Management, and Acquisition Logistics. His awards include The Defense Meritorious Civilian Service Medal, the Defense Exceptional Civilian Service Medal, and the Defense Superior Service Medal.

Mr. Harp, his wife, and family reside in Manassas, Virginia.

Dr. Paul D. Nielsen

**Director and Chief Executive Officer
of the Software Engineering Institute (SEI), Carnegie Mellon**

**Before the
United States House of Representatives
Defense Acquisition Reform Panel of the Committee on Armed Services**

**July 9, 2009
8:00 a.m.**

Written Statement of Dr. Paul Nielsen, Software Engineering Institute (SEI)
HASC Panel on Acquisition Reform
July 9, 2009

Chairman Andrews and Ranking Member Conaway, thank you for the opportunity to participate in this hearing before the Defense Acquisition Reform Panel of the Committee on Armed Services about the challenges facing effective acquisition and management of information technology systems. After serving in the Air Force for 32 years, including my final assignment as the commander of the Air Force Research Laboratory at Wright-Patterson Air Force Base in Ohio and after the past five years as the director of the Software Engineering Institute, I have experienced firsthand the challenges and opportunities that we face in defense acquisition.

Growth in Software Reliance

Today our military men and women train, operate and fight in a cyber environment that is based upon global IT architectures, applications and services. Gone are the days of IT being a support infrastructure to a few basic missions. Today and in the future, IT architectures and services have created and enabled the cyber environment within which a majority of key DOD missions and functions are conducted, for example: Command and Control, Operations, Logistics, Medical, Personnel Management, and Intelligence. Almost everything a soldier, sailor, marine or airmen does has some interaction with IT and software—from recruitment to retirement, from getting paid to getting medical help, from planning operations to executing them. So when the IT acquisition process and programs fail to deliver quality integrated architectures and systems that are reliable, assured, and secure – every major military mission is potentially impacted. And now, to further complicate both acquisition and operations, we all work in a global cyber environment with all the benefits and vulnerabilities of the connectivity enabled by our IT systems. So thank you for making IT acquisition the focus of this hearing.

The Carnegie Mellon Software Engineering Institute (SEI) is a Department of Defense Federally Funded Research and Development Center (FFRDC). Our work is centered on the software component of our systems, the core of their functions and capabilities – often totaling one third or more of the overall cost of an acquisition program. In fact, one of the largest challenges we see facing the Department of Defense is the effective management of the software foundation upon which all military platforms, capabilities and systems of systems are built and run. For operational success these capabilities must all function in real-time or near-real-time and are often networked. Our military can only operate at its peak capability with reliable, high quality, and secure information technology. Software is the heart of our command and control capabilities and services. It's the glue that connects our systems and integrates our systems. It's critical to the warfighter that our software intensive systems perform as flawlessly as possible.

Due to the levels of complexity that now exist in software development, engineering, and security, software is often the least understood and most neglected component of our DOD IT architectures today; and although major DOD systems encompass more than just software, it is the software that fundamentally allows them to function. Especially worrisome is that at present, and for the foreseeable future, both our global combat and peacekeeping engagements rely on software and systems that may contain components produced outside the United States.

The percentage of weapon system functionality that is dependent upon software has sky rocketed and will only continue to grow. Figure 1 shows this growing reliance on software for functionality in military aircraft:

Written Statement of Dr. Paul Nielsen, Software Engineering Institute (SEI)
 HASC Panel on Acquisition Reform
 July 9, 2009

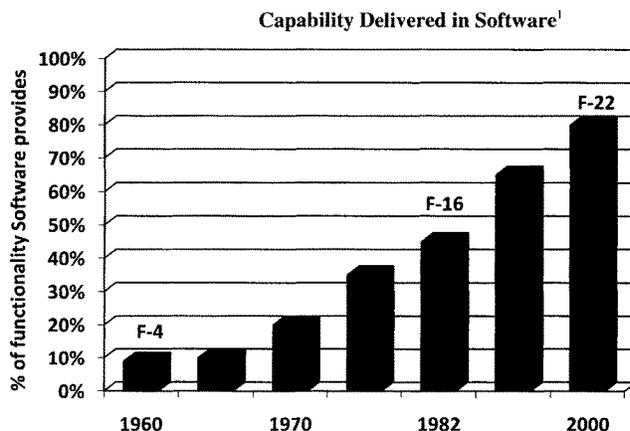


Figure 1

Why is Software Acquisition so Difficult?

The “unlimited” complexity of software is neither well understood nor well appreciated by many. Software is not rooted in the physical world like other engineering disciplines—civil, aeronautical, electrical, or mechanical engineering. Without physical constraints, the design space is so vast for large programs that you need strong architectural principles, disciplined processes, and talented people to be successful. The larger the program, the more important this is—and, as you are aware, many defense programs are very large.

Additionally, software is invisible; people don’t buy code - they acquire systems that satisfy requirements. And software is intangible—you can’t touch it or kick its tires. Nevertheless, in most defense systems, software is critical to the very success of the program. The systems just don’t work without software.

The challenges of acquiring software-reliant systems continue to grow along with their expanding functionality and complexity, but software code is rarely designed and produced entirely within an acquisition program any longer. We use a great deal of commercial off-the-shelf (COTS) software especially in our IT systems: commercial operating systems, data base software, enterprise business solutions, e-mail and office productivity software. The government has gained a lot of from the use of commercially available software. But now, in an era where we worry more about malicious code, we don’t always know where this commercial software was written, what support software and hardware was used to create it, and ultimately how trustworthy the code really is.

Without solid software engineering, software issues often don’t become evident until late in an acquisition, such as during integration and test, which results in significant program slips. With software and hardware technologies continuing to evolve rapidly, very few program managers — or key decision

¹ Watts S. Humphrey, *Winning with Software: An Executive Strategy* (Boston: Addison-Wesley 2002), 4

Written Statement of Dr. Paul Nielsen, Software Engineering Institute (SEI)
 HASC Panel on Acquisition Reform
 July 9, 2009

makers — have a deep understanding of software technology, even as demands increase for further integration, interoperability, system-of-systems capabilities, service oriented architectures, and cloud computing. Additionally, mounting expectations for software systems to be connected, configurable, and interoperable add to the challenges of ensuring their security.

In fact, the current challenges we face in software engineering and integration are daunting. In addition to core issues with standard and comprehensive acquisition policy and approaches, we face the development of extremely large systems with several million software lines of code (SLOC) that often utilize insecure and unassured software engineering. Amplifying development complexity is the creation of “hybrid” systems which integrate legacy re-use (a task often misconceived as being “easy”), COTS software, and new unverified technologies. Complications are further augmented when multi-contractor teams are using different software processes, dispersed engineering, and separated development and operational locations (to include ever growing software development in China and India) to complete developments.

Therefore a solid foundation for IT software acquisition includes not only the required technical expertise, management oversight and quality assurance processes but also the adequate budget, schedule, and staff needed to carry them out. Of course this is always a challenge due to pressured timelines and cost schedules. At the SEI we have presented a preliminary framework of activities focused on building security into the government’s major software reliant acquisition systems and architectures, spanning the acquisition life cycle from identification of a mission or business need to system delivery. We continue to work to refine this work to ensure our IT architectures and systems are based upon secure software of high quality.

Ten Key Reasons Software Acquisitions Fail

The SEI has almost 25 years of experience working with DOD and other government acquisition programs managing developments that include persistently growing amounts of increasingly complex software code. This experience provides the basis upon which we compiled this list of Ten Key Reasons Software Acquisitions, and systems which are software dependent, fail to meet their goals on time and/or on budget.

1. Technology key to program success is new to the organization
2. Software issues are considered too late in the system-development process
3. Inadequate planning and estimating
4. Size matters – large projects get into trouble more frequently than smaller ones, all projects grow larger over time
5. Software objectives are not fully understood or specified; they change frequently (and grow) during the project
6. Inadequate experiences and trained project management
7. Inadequate process emphasis and erosion of process discipline
8. Inadequate contract incentives to encourage use of proven software engineering practices
9. Acquirers and developers lack experience working as a team or the resources to do so
10. Insufficient senior staff and inexperienced software engineering cadre

How to Better Manage Large Software Efforts

Increasing focus on the following six steps would, in my opinion, significantly assist efforts to successfully manage the development of large software systems and software intensive systems.

Written Statement of Dr. Paul Nielsen, Software Engineering Institute (SEI)
 HASC Panel on Acquisition Reform
 July 9, 2009

1. Incorporate Software Early and Continuously in the Systems Engineering Process

Recognize that software represents a major risk and is a critical technology that needs to be watched like other technologies. It is vital to the success of a program that software engineering efforts start early as a key part of the systems engineering process. This means including software in early CONOPS, architecture, and requirements activities, (e.g., concept/trade studies). Competing demands on the budget between early adoption of good software engineering practices and “producing” something tangible can be alleviated by obtaining independent software cost and schedule estimates and maintaining an executable software cost, schedule, and requirements baseline. Software security and resiliency engineering must also be included early in development. Too often, software security receives insufficient attention in critical, early life cycle activities, leaving systems open to attack and putting the warfighter directly in harm’s way when systems are deployed.

One of the most troubling aspects of software development is that typically more than half of the development cycle is devoted to fixing errors, often not discovered until the system test. The cost to correct software errors – in both time and money – incrementally increases as the development stage advances. The rising costs of fixing defects late in the development cycle – or worse, after deployment to our warfighters – indicates the need for more effective development methods that avoid injecting errors or find them much earlier. The solution is to build quality in with effective software engineering—and do it from the beginning of the program.

2. Recruit and Develop a Trained Software Staff within the Program Office

To ensure personnel requirements, both in quality and quantity, can be met with acceptable staff, use professionals from the military, civil service, and Federally Funded Research and Development Centers (FFRDC) to help train, monitor and work with developmental contractors on architecture, design, and other issues. If possible, aim for a “critical mass” so software concerns have sufficient voice; ensuring personnel requirements are clearly identified, including stipulations that all software players should have the software architecture embedded in their thinking. To reduce software integration risk, verify that the other domain experts, especially systems engineering and management, have at least a “reading level” understanding of software engineering and establish a common understanding of crucial software concepts across the program.

Designate leadership – programs should have a chief software engineer, a chief software architect (one person cannot really do both) and a software security engineer. All three positions must be provided with the appropriate responsibility and authority. Their roles are as follows:

- Chief Software Engineer – day-to-day technical management: a project engineer devoted to software. (Analog : general contractor for a building)
- Chief Architect – responsible for formulating vision for form, function, and usage of software in system. (Analog: architect for an office building)
- Designated security engineering function- led by an experienced systems/software security engineer, within the program office. Someone to continuously identify threats and vulnerabilities in the emerging operational environment and solution space

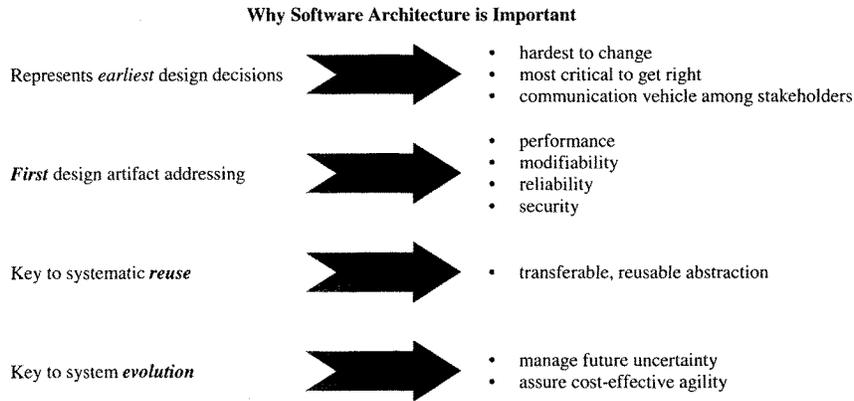
All science and engineering disciplines need men and women who are active and up to date in their field. It’s very important that government software professionals attend professional education classes and conferences. These events, most three to five days long, facilitate new ideas and approaches while helping these professionals improve and sustain their skills; but too often there are no funds for these activities.

Written Statement of Dr. Paul Nielsen, Software Engineering Institute (SEI)
 HASC Panel on Acquisition Reform
 July 9, 2009

3. Ensure Adequate Emphasis on Software Architecture

In recent studies by OSD, the National Research Council, NASA, and the NDIA, architectural issues were identified as a systemic cause of software problems in DOD systems.

Poorly designed software architectures result in greatly inflated integration and test costs and an inability to sustain systems in a timely and affordable manner. Furthermore, without the right architecture, systems will not only lack robustness but will likely exhibit undesired, disparate behaviors at the system and system-of-systems levels. No one would attempt to build a home or a major office building without an architect and without several architectural views, but time and again not enough time and effort are spent on the software and system architectures of our defense programs.



The **RIGHT ARCHITECTURE** paves the way for system **SUCCESS**.
 The **WRONG ARCHITECTURE** usually spells some form of **DISASTER**

Figure 2

Software architecture drives software development throughout the life cycle and therefore must be central to software development activities. To design a software architecture that satisfies constraints, meets functional requirements, and fulfills key quality attributes, it is imperative that the appropriate stakeholders are involved throughout to ensure both mission and business goals are used to explicitly identify and characterize fundamental features. Assuring adequate consideration is given to all of the quality attributes including safety and security, will result in a more robust and resilient system.

4. Software Security Must be a Main Concern

Many systems are designed and developed with little initial concern for the software's security properties, directly increasing the danger and exposure for users. Security is seen as a patch not a design feature. This situation is made even worse by the trend that more software development is being outsourced off-shore. Commercially available software is often delivered with unintentional security vulnerabilities due to defects and, occasionally, with hidden malware—purposely designed vulnerabilities.

Written Statement of Dr. Paul Nielsen, Software Engineering Institute (SEI)
 HASC Panel on Acquisition Reform
 July 9, 2009

This is due, in part, to the lack of emphasis on security as an integral part of software in the acquisition process, including the lack of accountability for acquisition officials to verify software assurance. The rampant worldwide increase in exploitation of software vulnerabilities demands that development practices minimize software errors and other vulnerabilities that give our adversaries an open door to exfiltrate data and to deny or degrade services.

Today's software engineering practices permit dangerous error, whether they are introduced by mistake, poor practices, or with the intent to cause harm; enabling hundreds of attack programs to compromise millions of computers every year. Software is an underpinning of all critical infrastructures, including public systems such as health IT, energy, and banking and finance. Exacerbating the problem are the advanced and persistent cyber threats that are increasingly targeting our defense industrial base.

As our adversaries—both foreign and domestic—become increasingly sophisticated in their ability to insert malicious code into critical software we must work to minimize their ability to introduce and exploit vulnerabilities.²

5. Establish an Effective Process

"History has shown a direct relationship between the effectiveness of the processes used to manage a project and how well that project meets its cost, schedule, and performance objectives—projects with strong processes have a far greater probability of meeting their objectives than projects that have weak processes. These disciplined processes are based on the best practices identified by the Software Engineering Institute (SEI) ... and other experts, which have been proven to reduce the risk in implementing systems." — General Accounting Office³

A well established process can help programs support the goals of the military by enabling repeatability, insight and oversight, control and tracking, measurement, improvement, training and transformation (via consistency, integration, coordination). Using the right processes to manage and develop software can dramatically reduce the risk of acquiring software-intensive systems. For it is just as true for software, as it is in many other high-tech industries, that measured and managed processes, designed and tailored to support the development of a system, provide the best possible performance for a given workforce and technology. Our research has shown that the right process improves the predictability of development cost and schedule, as well as the quality and reliability of delivered systems. It reduces time to field, lowers development and ownership costs, and increases the probability of mission success by providing early warning of issues while there is still time to act. Both the acquirer's and the supplier's ability to achieve a successful outcome are improved, and the greatest positive impact is realized when best practices are applied across all the engineering domains, including acquisition, in every stage of development.

For success, action plans should be established early to increase efficiency and effectiveness of program processes as well as produce measured progress. Interactions between multiple government and contractor stakeholders should be considered as high risk areas. The key is not so much about having the "best process," it's about having the *right* process to deliver the right capability to the warfighter when they need it.

² The Department of Defense (DOD) and Department of Homeland Security (DHS) Software Assurance (SwA) Acquisition Working Group, *Software Assurance in Acquisition: Mitigating Risks to the Enterprise, A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing*, October 22, 2008

³ GAO-07-1157R DHS Posthearing Questions

Written Statement of Dr. Paul Nielsen, Software Engineering Institute (SEI)
HASC Panel on Acquisition Reform
July 9, 2009

Benefits of Process

We continuously study and evaluate the improvements organizations have seen when they focus on disciplined development so that we may better understand and advance software engineering best practice. We have provided the committee some of the resultant reports showing the benefits, but summarizing from these reports (Figure 3), we know that dramatic improvements in cost, schedule, predictability, and the quality of delivered software can and have been achieved, and that the return on investment (Figure 4) for these results is rapid and significant.⁴

Measured Benefits Utilizing Process

Benefit Measured ³	Median Improvement
Cost	38%
Schedule	50%
Quality	50%
Customer Satisfaction	14%
Return on Investment	3:1

Figure 3

Process Improvement Pay-Off⁶:

Data Source	Process Improvement	ROI/Benefit Conclusions
Raytheon study of multi-site internal improvement effort	Implementing SW CMM and migrating to CMMI	<ul style="list-style-type: none"> • 36% drop in Cost-Performance Index variability • 70% drop in Schedule Performance Index variability • Continuous productivity gains: 1997-1999 - 30%; 2000 - 9%; 2001 - 11%; 2002 - 6%
US Air Force F-16 Logistics Operations Division - AFMC	Processes for defect analysis and removal to reduce Operations and Sustainment (O&S) costs	<ul style="list-style-type: none"> • \$43 M in documented sustainment cost savings (2002) • \$900 M projected savings for the life of F-16 program
DACS (on behalf of DOD)	Review of commercial and government process improvement results and ROI for measured defect identification and removal, reduced rework, increased productivity, decreased cycle time, etc	<ul style="list-style-type: none"> • 54% Fewer validation cycles (Schlumberger) • 100% Productivity Increase (Schlumberger) • 51% Increase in on-time delivery (Schlumberger) • 25% Post-release defects ((Schlumberger) • Most defects eliminated before testing (Boeing STS) • 31% Reduced rework -- 7.75:1 ROI (Boeing STS) • 55% Reduced software development costs (NASA SEL) • 40% Decreased cycle time (NASA SEL)

Figure 4

⁴ JWO suggestions for this list include CMU/SEI-2003-TR-009, CMU/SEI-2003-TR-014, CMU/SEI-2006-TR-004, CMU/SEI-2007-TR-013

³Source for this table is CMU/SEI-2006-TR-004

⁶ Source - Benefits of Improvement Efforts, CMU/SEI-2004-SR-010, Oct 2004

Written Statement of Dr. Paul Nielsen, Software Engineering Institute (SEI)
HASC Panel on Acquisition Reform
July 9, 2009

6. Continued Software Engineering, Research and Development

Software engineering is a relatively new discipline, subject to ongoing and immediate advances in capability, constantly changing to support the development of larger and more complicated systems, guaranteeing that what is “effective” or “right” today will not be appropriate in the future. Therefore, it is essential for the DOD to continue to work to establish and incentivize the adoption of the most effective practices and processes available.

In an endlessly evolving world it is crucial to US security and future operations that we fund the necessary research to meet the increasing demands of the warfighter and at the same time stay ahead of our adversaries, whose capabilities and tradecraft transform daily. The commercial world will continue to invest in technologies and innovations for which they can see a business case, but they will not always have a complete overlap on military requirements. The military often works in very hostile and remote environments, lives depend on its systems, and the nation’s success in meeting its goals and objectives are enabled by its systems. It is very important that the DOD invest in research in software engineering with an eye on its unique requirements.

In conclusion, none of these techniques are “silver bullets.” Acquisition is a “team sport” and the development of complex systems of systems demands an acquisition team with a capable acquisition manager teamed with capable development managers. The team includes the senior acquisition officials in the Pentagon—and the appropriate congressional committees. We all have a responsibility to the soldiers, sailors, marines and airmen to support them with affordable, secure, operable systems that meet the nation’s needs.

I would like again to thank the Committee for providing me the opportunity to testify on this topic of critical importance to our Nation and the Department of Defense.

Biography: Paul D. Nielsen



Dr. Paul D. Nielsen is Director and Chief Executive Officer of the Software Engineering Institute (SEI), a Federally Funded Research and Development Center operated by Carnegie Mellon University. The SEI advances software engineering principles and practices through focused research and development, which is transitioned to the broad software engineering community.

The SEI serves as a global leader in process improvement and networked systems survivability. Additionally, the SEI is a key innovator in software architecture, software product lines, interoperability, the integration of software intensive systems, and the increasing overlap of software and systems engineering. The SEI also provides direct support to more than 50 US government agencies in their efforts to efficiently and effectively acquire new software and systems.

Since joining the SEI in August 2004, Nielsen has overseen the development and expansion of the CMMI product suite, the establishment of new SEI offices in Qatar, and the growth of the SEI to an organization employing more than 500 employees with operating revenues of \$100 million annually.

Prior to his arrival as SEI Director, Nielsen served in the U.S. Air Force, retiring as a Major General after 32 years of distinguished service. As commander of the Air Force Research Laboratory at Wright-Patterson Air Force Base in Ohio for more than four years, he managed the Air Force's science and technology budget of more than \$3 billion annually. He also served as the Air Force's technology executive officer, determining the investment strategy for the full spectrum of Air Force science and technology activities.

Nielsen's Air Force career includes assignments at the Secretary of the Air Force's Office of Special Projects and the Department of Energy's Lawrence Livermore National Laboratory. Nielsen was a military assistant in the Office of the Secretary of Defense and the Commander of Rome Laboratory. He was Operations Chief for the Cheyenne Mountain Operations Center and Director of Plans for the North American Aerospace Defense Command. Prior to his assignment at the Air Force Research Laboratory, Nielsen served as Vice Commander of the Aeronautical Systems Center, the Air Force's largest product center responsible for developing fighters, bombers, transports, reconnaissance aircraft, training systems, and unmanned aerospace vehicles.

In 2004, Nielsen became a Fellow of the American Institute of Aeronautics and Astronautics (AIAA). He served as the AIAA President from 2007-2008 and is a member of the AIAA Board of Directors. In 2006, he was elected as a Fellow of the Institute of Electrical and Electronic Engineers (IEEE). Nielsen serves on the Air Force Scientific Advisory Board and is a member of the Board of Directors for the Hertz Foundation, a non-profit that awards graduate school fellowships in the applied sciences.

Education

- BS, U.S. Air Force Academy
- MS, University of California, Davis
- MBA, University of New Mexico
- PhD, University of California, Davis

**DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION**

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(4), of the Rules of the U.S. House of Representatives for the 111th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Armed Services Committee in complying with the House rule.

Witness name: Dr. Paul Nielsen

Capacity in which appearing: (check one)

Individual

Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: Carnegie Mellon University's Software Engineering Institute

FISCAL YEAR 2009

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
1 Federal Contract	Under Secretary of Defense for Acquisition, Technology and Logistics, USD(AT&L)	\$63,651,328 YTD	Provides technical leadership to advance the practice of software engineering so that DOD can acquire and sustain its systems with predictable and improved cost, schedule, and quality

FISCAL YEAR 2008

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
1Federal Contract	Under Secretary of Defense for Acquisition, Technology and Logistics, USD(AT&L)	\$76,208,172	Provides technical leadership to advance the practice of software engineering so that DOD can acquire and sustain its systems with predictable and improved cost, schedule, and quality

FISCAL YEAR 2007

Federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
1Federal Contract	Under Secretary of Defense for Acquisition, Technology and Logistics, USD(AT&L)	\$60,837,489	Provides technical leadership to advance the practice of software engineering so that DOD can acquire and sustain its systems with predictable and improved cost, schedule, and quality

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2009): 1 Federal Contract _____;
Fiscal year 2008: 1 Federal Contract _____;
Fiscal year 2007: 1 Federal Contract _____.

Federal agencies with which federal contracts are held:

Current fiscal year (2009): Under Secretary of Defense for Acquisition, Technology and Logistics USD(AT&L) _____;
Fiscal year 2008: Under Secretary of Defense for Acquisition, Technology and Logistics USD(AT&L) _____;
Fiscal year 2007: Under Secretary of Defense for Acquisition, Technology and Logistics USD(AT&L) _____.

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2009): Provides technical leadership to advance the practice of software engineering so that DOD can acquire and sustain its systems with predictable and improved cost, schedule, and quality.

Fiscal year 2008: Provides technical leadership to advance the practice of software engineering so that DOD can acquire and sustain its systems with predictable and improved cost, schedule, and quality.

Fiscal year 2007: Provides technical leadership to advance the practice of software engineering so that DOD can acquire and sustain its systems with predictable and improved cost, schedule, and quality.
_____.

Aggregate dollar value of federal contracts held:

Current fiscal year (2009): \$63,651,328 YTD

Fiscal year 2008: \$76,208,172 _____;
Fiscal year 2007: \$60,837,489 _____.

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2009): N/A _____;
Fiscal year 2008: N/A _____;
Fiscal year 2007: N/A _____.

Federal agencies with which federal grants are held:

Current fiscal year (2009): _____;
Fiscal year 2008: _____;
Fiscal year 2007: _____.

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2009): _____;
Fiscal year 2008: _____;
Fiscal year 2007: _____.

Aggregate dollar value of federal grants held:

Current fiscal year (2009): _____;
Fiscal year 2008: _____;
Fiscal year 2007: _____.

Testimony before the House Armed Services Committee Panel on Defense Acquisition Reform

Ronald L. Kerber

Introduction

It is my pleasure to testify before the House Armed Services Committee Panel on Defense Acquisition Reform. My name is Ronald Kerber and I am appearing before you as a member of the Defense Science Board (DSB). As a member of the Board, I led three task forces that inform my testimony today. I must also state that the views expressed today may or may not represent the official views of the Department of Defense. I was asked to pay special attention to the Defense Science Board findings “especially as they pertain to ‘root causes’ or system problems inhibiting our ability to effectively acquire IT systems.” My testimony is supported by three Defense Science Board reports:¹

- *Department of Defense Policies and Procedures for the Acquisition of Information Technology*, March, 2009
- *Creating a DOD Strategic Acquisition Platform*, April 2009
- *Information Management for Net-Centric Operations*, April 2007

I will break my testimony into two parts. Part 1 will deal with general issues pertaining to the Department of Defense (DOD) acquisition process. Part 2 focuses on issues peculiar to the acquisition of information technology.

General Acquisition Process Issues

Fixing the DOD acquisition process is a national security issue.

Today, the defense acquisition process takes too long to produce weapons that are too expensive and often technically outdated by the time they are fielded. Typical major system acquisitions take 10–15 years, while new product development in the commercial sector of similarly complex systems takes one third to one half of that time. Acquisition of information technology, on which many defense systems are

1. Copies of these reports have been provided to the Committee.

critically dependent, also exceeds typical commercial development time—taking three to four times as long. These development times are far outpaced by the rapid advances in technology, which means that subsystems can be one or two generations old by the time a system is provided to war fighters in the field—unless upgrades are incorporated before the system is fielded. Furthermore, programs often have large cost overruns, long schedule delays, and unsatisfactory product quality and performance.

At the same time, the nation faces very adaptive adversaries. The United States is no longer in a unique position of technological supremacy. Many types of advanced technology are readily available on the world market. Adversaries are becoming very adept at fashioning new weapon capabilities from commercially available technology—“good enough” systems are developed and fielded quickly. And, these adversaries are often far more agile in doing so than is the United States. Most military planners recognize that a robust military strategy combines a formidable offense with a capable and comprehensive defense. But some current adversaries can target U.S. vulnerabilities and time their attack without concern for the risk of U.S. offensive retaliation—as they have little of value to put at risk. Adaptive adversaries are able to identify U.S. vulnerabilities and create effective systems to exploit them—one example is improvised explosive devices that became prominent early in the Iraq conflict and continue to plague U.S. forces. When rogue states and terrorists employ this strategy, it creates a particular challenge for the nation. Thus, we too must be able to more rapidly and effectively transition commercial and military-unique products to our war fighters in the field.

While this scenario applies to all weapon systems, information technology presents a somewhat different set of challenges due in large measure to the fact that it is an important enabler for so many defense capabilities. It underlies the nation’s ability to gain better intelligence, better situational awareness of the battlefield, better communications, and more precision in weapon system delivery. In fact, the use of information technology is pervasive, from administrative systems for managing business processes, to embedded subsystems in major weapon systems—comprising as much as 90 percent of the cost of some new systems.

Despite its crucial importance, the Department’s ability to acquire information technology is fraught with problems. Driven by the short half-life of commercial information technology, hardware supportability, software applications, and evolving operational requirements, continuous upgrades and product improvement are a reality that must be accommodated by the acquisition process. In addition, it is often difficult to technically validate these programs to ensure that what is being delivered is in fact what is expected, raising the potential for unknown system vulnerabilities.

Furthermore, many information technology systems are managed as joint programs, ultimately used by more than one of the military services. Systems such as intelligence, surveillance and reconnaissance; command and control; and communication systems are often acquired as joint programs to ensure interoperability and common fielding dates among the user services. As a result, managing these programs requires joint cooperation among the services—something that can become a challenge to effective acquisition. Stable budgets and system interoperability—that is, systems developed to operate with many others on the battlefield—are challenging criteria that can be difficult to achieve and remain important issues.

Finally, the acquisition of services receives far less attention than that of materiel, yet it is a growing part of the defense budget—representing about 50 percent of the acquisition budget. Services range from support to the battlefield, to airlift and logistics, to security services, janitorial services, studies and analysis and information technology support services. Such activities are not only necessary but also smart to contract as services so that DOD personnel can devote their time to the jobs they were trained to do. Yet it is still reasonable to ask whether all such contracts are necessary and whether they could be contracted more efficiently. Service contracts should be subjected to the scrutiny and be required to meet certain criteria similar to materiel acquisition.

The problems of acquisition execution outlined above have been well known for years. Yet an even more important deficiency is the process that determines what to buy. The strategic plan for acquiring military capabilities is only loosely aligned with national security objectives and the military missions to achieve them. The military services are tasked to train and equip the nation's forces and they often control the input into the process—defining the capabilities to be acquired. The combatant commanders, who actually use forces and equipment in the field to execute missions, have little input into what next-generation capability will be acquired. Often present programs reflect past missions and seldom adequately support joint needs, despite the fact that ongoing combat experiences demonstrate new joint needs and interoperability issues. Clearly the driving agenda item that the Department needs to address is the process that determines what to buy to support the highest priority national security mission needs.

The shortcomings addressed here point to an acquisition process that is inadequate to meet the needs of the Department of Defense. Fixing this process must become a departmental priority—led by the Secretary of Defense.

There have been many attempts to fix the acquisition process, but none, as of yet, have been successful.

The defense acquisition process has been studied for decades—by the Packard Commission, the Government Accountability Office, the Defense Science Board, think tanks, commissions, and many other organizations, including the Department itself. For decades, these studies have identified numerous flaws—problems with bureaucracy, accountability, overlap of authority, inefficient processes, and inexperienced leadership. And over the years, the Department has made a series of attempts to “fix” acquisition—usually at the direction of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Yet problems persist—major system acquisitions still take too long, costs are overrun, and concerns remain over product performance and quality.

Why have previous efforts so often failed? In part, it is because they fail to address the root causes of the problem, focusing instead on re-engineering the mechanics of the acquisition decision process. Many problems appear to be caused by the use of immature technology, requirements “creep,” or funding instability. **Such problems, however, are really only symptoms of the lack of experienced judgment on the part of Department personnel who structure acquisition programs in a way that will almost certainly lead to failure.**

Moreover, many organizations in DOD are often not aligned with departmental acquisition goals and objectives. The staff of the Office of the Secretary of Defense—including the Director, Program Analysis and Evaluation; the Comptroller; the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer; Director, Defense Research and Engineering; and Director, Operational Test and Evaluation—the military services, and the Joint Staff are all power centers that not only often fail to be aligned with each other, but sometimes are not even aligned within themselves. Hence, many of the Secretary’s advisory staff, who are not accountable for delivering acquisitions, can stall a program’s ability to proceed through the process while awaiting their input.

Perhaps the most important reason that previous efforts have failed, however, is that the problem has been left to the Under Secretary of Defense for Acquisition, Technology, and Logistics. But the acquisition challenge is much bigger and broader than the authority or scope of power of that office. Many of the organizations, functions, and processes that support acquisition are not, and should not be, the responsibility of the acquisition under secretary. Fixing defense acquisition is a challenge that can only be successfully addressed by the Secretary of Defense, and it should be among his top priorities. The Secretary not only must lead the charge within DOD to fix the acquisition process but also must inform the Congress of

departmental actions and enlist its support for his agenda, least Congress act independently in a way that undermines his efforts.

There is no silver bullet for “fixing” acquisition. As noted previously, many studies have identified many problems and offered many solutions. One particular difference in the findings and recommendations drawn from a decade of past studies by the Defense Science Board is in how the problem is defined. Fixing acquisition challenges must begin with leadership action by the Secretary of Defense. And it must address not only “how” the Department buys material but also “what” materiel the Department buys, who is involved in the process, and whether support systems help or hinder.

The Secretary of Defense must create a strategic acquisition management platform comprised of four critical elements.

1. Buy the right things.

The strategic military planning system, DOD’s regime for deciding “what to buy,” has a weak analytic foundation. When we buy the wrong thing, we blame the acquisition system. But that system is responsible for “how to buy.” Before fixing the acquisition processes, the Secretary must reform the strategic military planning system and create a genuine “business plan” for DOD. The plan should be developed with greater involvement of the regional combatant commands and better use of systems engineering and of modeling and simulation.

2. Select an effective leadership team.

Proven, relevant experience is needed in the Office of the Secretary of Defense, the military departments, and defense agencies. Today, many people are inexperienced, from leadership to program managers. Few have a personal track record of repeated successes at acquisition. Trial-and-error and on-the-job training can be really expensive. The Department needs to hire and assign individuals with proven records of acquisition success. This may mean facing the possibility of not doing a program until the right people are available. In order to determine the “right size” for the acquisition workforce, the Department can use process mapping and work flow analysis to determine the necessary functional staffing and to eliminate overlapping accountability and authority which leads to excessive bureaucracy.

3. Reform and streamline the acquisition process.

A single acquisition process cannot meet the needs for acquiring major systems, commercial derivatives, and information technology systems, and to rapidly field critical war fighting needs in time of crisis. The process to buy major systems, information technology systems, and commercial derivatives

needs to be streamlined with up front, strong systems engineering support. The case of information technology presents unique challenges—in stand-alone systems, embedded systems, and net-centric infrastructure. A new system is needed that recognizes the rapid advances in information technology and plans for frequent and efficient upgrades after delivery. Fielding critical war fighting needs in time of conflict also requires a new approach—a standing acquisition capability that can fulfill these requirements in a timely way, as there is little doubt that the need will continue.

4. Improve acquisition execution.

Acquisition improvements are not enabled by policy and process reforms alone. They must be coupled by efficient, effective execution. Key areas where improvement in management and execution are needed include: product development management, contract award and management, acquisition workforce, acquisition integrity, and process metrics. Central to these improvements is experienced personnel with reinforcing incentives—in leadership, in the acquisition workforce, and, equally important, in the contractor base. Up front attention to systems engineering during product development as well as keen attention to acquisition integrity are also essential ingredients.

Many may say that they are already doing what is recommended here. In fact the recommendations are essentially common sense and one may find each concept used in an isolated case. The real message presented is that a comprehensive approach must be used uniformly across the defense enterprise to be successful. In fact if "they were already doing this" comprehensively there would be no problem or need for your Panel.

Issues Peculiar to the Acquisition of Information Technology

Information technology (IT) offers immense capability in terms of agility, flexibility, responsiveness, and effectiveness. It enables nearly all of our military combat capability and has become a necessary element of our most critical warfare systems. However, there is growing concern within Congress and among DOD leadership that the nation's military advantage may be eroding. The deliberate process through which weapon systems and information technology are acquired by DOD cannot keep pace with the speed at which new capabilities are being introduced in today's information age—and the speed with which potential adversaries can procure, adapt, and employ those same capabilities against the United States.

Certainly, barriers that preclude transformation of the U.S. national security apparatus to meet the challenges of a new strategic era are of particular concern. Nearly a decade ago the Department established a vision for the architecture and structure for information system management—a vision that is still evolving. However, it is well known that acquisition has not been well managed for these systems within this “enterprise level” construct, and the result has not served today’s leaders and soldiers well. In fact, it hinders the war fighters’ ability to use information technology to its fullest potential for situation awareness, collaboration, and rapid decision-making. The resulting operational impact is profound.

Yet despite the current situation, successful programs exist that comprise largely or exclusively of information technologies or are deeply dependent on information technology in execution. The question then arises as to whether there are elements common to the acquisition of these successful programs that would improve the Department’s ability to field advantageous information technology in a timely and cost-effective manner.

Recently, acquisition policy was again modified in part to add more rigor and discipline in the early part of the acquisition process. Likewise, the Joint Capabilities Integration and Development System (JCIDS) Instruction and Manual are being updated with changes to the Joint Staff’s oversight and governance of IT programs. These policies derive from a single acquisition model that applies to both major automated information systems and major defense weapon systems acquisition programs.

Information technology is pervasive in weapon systems as well as defense business systems. In its contributions to both functionality and cost, information technology now represents a considerable proportion of all acquisition programs underway today—a proportion that is likely to increase in the future. Thus, whether existing DOD acquisition policies and processes provide the foundation for an effective information technology acquisition model is a critical question for the Department—one that deserves special attention from the Secretary of Defense.

At the request of Congress, the Defense Science Board undertook a review of Department of Defense policies and procedures for the acquisition of information technology. The findings and recommendations, presented in the *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology*, are the result of a study that was broad in scope, as established in legislative guidance—covering acquisition and oversight policies and procedures, roles and responsibilities for acquisition officials department-wide, and reporting requirements and testing as they relate to information technology acquisition.

A key finding of the DSB review is **that there is a need for a unique acquisition system for information technology**. Such a process must be designed to accommodate the rapid evolution of information technologies; their increasingly critical position in DOD warfare systems, warfare support systems, and business systems; and the ever evolving and often urgent IT needs of the war fighter. The current conventional process, with its recent improvements, would be used when a system requires significant scientific or engineering technology development, particularly hardware development or the integration of many complex systems requiring design and functionality partitioning and trade-offs.

Problems that plague IT acquisition are similar to those that plague the acquisition of major systems, most of which have a high content of embedded IT. **The conventional DOD acquisition process is too long and too cumbersome to fit the needs of the many systems that require continuous changes and upgrades**—a reality driven by the short half-life of commercial information technology, supportability of hardware (which is often a commodity), software applications, and operational requirements. Thus, the Department's leaders must take action to address this problem. Toward that end, the DSB task force offered the following recommendations to change the Department's approach to information technology acquisition.

Statutory Restrictions

The task force believes that the statutory framework is workable and is not a major impediment to improving IT acquisition within DOD. Therefore, no recommendations are offered in this area. The main issue with regard to statutory influence is that Congress has lost confidence in DOD's execution of IT programs, which has resulted in increasing program scrutiny and budget actions (generally funding cuts) for programs that are faltering. Since DOD implementation of IT acquisition has fallen short, Congress has added additional constraints on reporting and management, these could become problematic when and if DOD begins executing programs well.

Acquisition Policies

Acquisition policies (DOD Directive 5000.1 and Instruction 5000.02) are principally designed for programs where technology development for hardware and software is a critical component. The recent revisions to DOD Instruction 5000.02, implemented December 2008, offer improvements to the process but do not address the fundamental challenges of acquiring information technology for its range of uses in DOD. Instead, a new acquisition approach is needed that is consistent with rapid IT development cycles and software-dominated acquisitions.

RECOMMENDATION 1. NEW ACQUISITION PROCESS FOR INFORMATION TECHNOLOGY

The Secretary of Defense should:

- Recognize that the current acquisition process for information technology is ineffective. Delays and cost growth for acquisition of both major weapons systems and information management systems create an unacceptable risk to national security.
- Direct the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)) and the Vice Chairman, Joint Chiefs of Staff to develop new acquisition and requirements (capabilities) development processes for information technology systems. These processes should be applicable to business systems, information infrastructure, command and control, ISR (intelligence, surveillance, and reconnaissance) systems, embedded IT in weapon systems, and IT upgrades to fielded systems.
- Direct that ALL personnel within the Office of the Secretary of Defense (OSD), the Joint Staff, and the Services and agencies involved with acquisition be accountable to ensure that their efforts are focused on the improvement, streamlining, and success of the new process.

The DSB proposes a new process, modeled on successful commercial practices, for the rapid acquisition and continuous upgrade and improvement of IT capabilities (Figure 1). The process is agile, is geared to delivering meaningful increments of capability in approximately 18 months or less, and leverages the advantages of modern IT practices. Multiple, rapidly executed releases of capability allow requirements to be prioritized based on need and technical readiness, allow early operational release of capability, and offer the ability to adapt and accommodate changes driven by field experience.

The process requires active engagement of the users (requirements) community throughout the acquisition process, with requirements constructed in an enterprise-wide context. It is envisioned that requirements will evolve so “desired capabilities” can be traded off against cost and initial operational capability to deliver the best capability to the field in a timely manner. A modular, open-systems methodology is required, with heavy emphasis on “design for change,” in order to rapidly adapt to changing circumstances. Importantly, the process needs to be supported by highly capable, standing infrastructure comprising robust systems engineering, model-driven capability definition, and implementation assessments—to reduce risk, speed progress, and increase the overall likelihood of repeated successes. Early, successive prototyping is needed to support the evolutionary approach. In addition, key

stakeholders—the Chief Information Officer (CIO), Program Analysis and Evaluation (PA&E), Director of Defense Research and Engineering (DDR&E), and Operational Test and Evaluation (OT&E), the Comptroller, operational users, and others—need to be involved early in the process, prior to the milestone build decision.

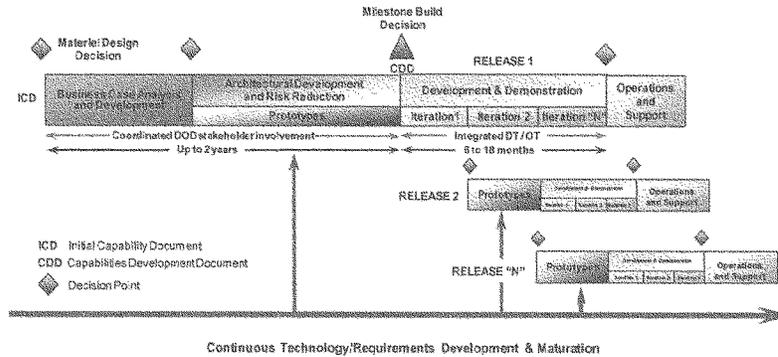


Figure 1. A New Acquisition Process for Information Technology

Testing methodologies and procedures need to be engaged early and often in the acquisition process, with integrated and continuous development and operational test practiced during the development and demonstration phase for each capability release. Contracting vehicles need to be devised that are flexible enough to support this agile process. These vehicles must allow for changes in delivered capability within a particular increment as well as allow capability to be deferred to subsequent increments if needed. Crucial to the success of a new process is continuity of funding, so as to maintain a solid funding stream for following, sometimes overlapping, capability releases.

Along with the flexibility built into the process, relevant metrics, similar to those used in commercial practice, are needed to continuously track IT acquisitions to ensure that the expected capability is being provided, costs are being managed, and the schedule to initial capability is on track. Finally, just as there is no substitute for acquisition leadership experience in DOD; the same is true for the contractor community. For contract award, program managers need to strongly consider relevant contractor experience and past performance, especially in large acquisitions, and ensure that key personnel are committed for the duration of the project.

This new process will have applicability over a broad range of new DOD IT acquisitions and upgrades to existing national security systems (including command and control systems), IT infrastructure, and other information systems (Figure 2).

Information technology is not simply a niche consideration—it touches a wide range of systems and, in turn, enables a wide range of capabilities.

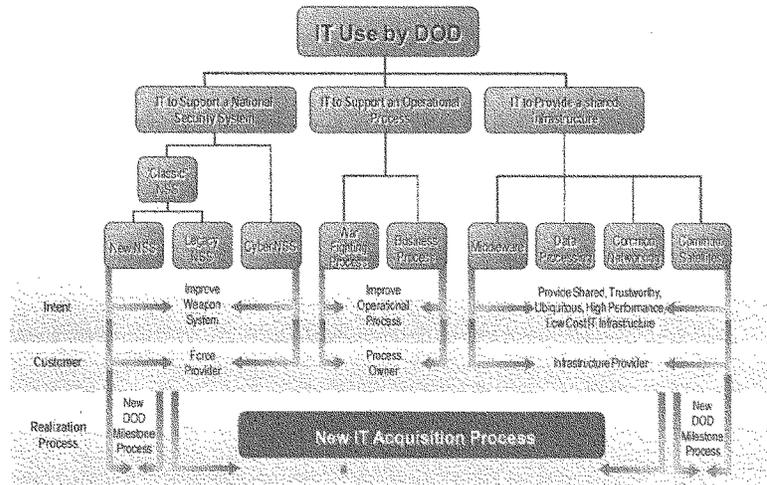


Figure 2. An Information Technology Acquisition Framework

Deciding When to Use the New IT Acquisition Process

It is important to clarify when to use the new IT acquisition process versus the improved DOD 5000.02 process for major weapon systems and communication satellites. In addition, it is also necessary to reduce potential confusion about technology development.

The use of the improved DOD 5000.02 process for major weapon systems is required when there are many design tradeoffs for both hardware and IT systems and for partitioning the functions and interoperability of embedded IT systems and subsystems in the new system, while assuring interoperability and network compatibility with the larger enterprise. At the same time there are likely to be areas of needed technology development that require advances in science and engineering that have little or nothing to do with IT—such as new material properties, increased speed, or stealth. This later scientific and engineering technology development should not be confused with the traditional jargon of the IT community that defines technology development nearly interchangeably with software development and hardware integration.

The use of the new information technology acquisition process is for new or replacement stand alone IT systems and subsystems, or for replacement IT systems embedded in existing weapon systems that are to be upgraded when there is little or no change in the hardware not associated with IT. It may also be appropriate to use the new IT acquisition system process concept within the 5000.02 process for new embedded IT systems in a major weapon system acquisition as the information technology could otherwise be a few generations old when the system is fielded.

While one could argue that the required decision as to which acquisition process to use could add confusion, one could also argue that if the leadership and program managers cannot sort out this high-level decision they have no chance of effectively managing or overseeing the program.

Roles and Responsibilities of the ASD (NII)/DOD CIO

Developing and implementing an acquisition process for information technology is an important step toward reducing delays and cost growth in information technology programs, as well as providing capability more rapidly to the war fighter. Perhaps equally important, however, is clarifying roles and responsibilities of the key players in the process—chief information officers and those individuals who hold milestone decision authority (discussed in the next section).

The DOD CIO function is currently housed in the Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (OASD (NII)/DOD CIO). DOD CIO responsibilities are delineated within titles 10, 40, and 44 of the U.S. Code. As designated in legislation, the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD (NII)/DOD CIO) reports directly to the Secretary of Defense—a reporting chain that is critical and must continue in order for the ASD (NII)/DOD CIO to have the necessary authority to carry out important department-wide functions.

The ASD (NII)/DOD CIO should have strong authority and responsibility for information policy vision, architecture, infrastructure, standards, spectrum, information assurance, interoperability, and enterprise-wide systems engineering. The ASD (NII)/DOD CIO should be the Department's single authority for certifying that IT acquisitions comply with an enterprise-wide architecture and should continually review ongoing programs for architectural compliance. He or she should also be a ruthless designer of "the enterprise" infrastructure and should approve IT program manager training and certification.

These functions are also applicable to CIOs at the Service and agency level. To execute the above responsibilities, Service and agency CIOs should also directly report to the head of the Service or agency, as required by legislation.

RECOMMENDATION 2. ASD (NII)/DOD CIO RESPONSIBILITIES

The ASD (NII)/DOD CIO should actively exercise his or her authority to certify that all IT acquisitions are consistent with the Department's net-centric architecture.

The ASD (NII)/DOD CIO should have strong authority and responsibility for enterprise-wide information policy vision, architecture, infrastructure, meta data and other standards, spectrum, interoperability, information assurance, and system engineering.

Certain capabilities in the OASD (NII)/DOD CIO must be strengthened in order to more effectively execute these responsibilities—in particular, system engineering, information assurance, and network integration.

In the Services and agencies, the CIOs should also have strong authorities and responsibilities for system certification, compliance, applications development, and innovation.

All CIOs should approve IT acquisition program manager training and certification and advise the personnel selection process.

The DOD CIO, supported by CIOs in the Services and agencies, should be responsible for certifying that systems and capabilities added to the enterprise do not introduce avoidable vulnerabilities that can be exploited by adversaries.

Both system vulnerability to sophisticated adversary threats and information and mission assurance should be addressed throughout program development, particularly in the early stages during the business case analysis and development phase. As new capabilities, infrastructure, and applications are added to a system, this same assessment should be continuously monitored with particular emphasis on source code analysis and supply chain risk assessment. A robust testing program must also be established to minimize the introduction of new vulnerabilities. New capabilities need to be tested in realistic test beds under a variety of threat scenarios.

Information and mission assurance must be an integral element of the IT acquisition process, not an afterthought. Information technology is far too important to the Department's war fighting and business endeavors to neglect information and mission assurance, as the consequences of doing so can undermine not only the current system but also other connected capabilities as well. In this context, it is instructive to remember that there is no way to test a large IT system to assure that

you “got what you wanted” and only what you wanted. Thus, since it is not possible to assure that an IT system is entirely safe and reliable, operators (combatant commanders) must develop field testing procedures; tactics, techniques, and procedures; and concepts of operations to test system authenticity and operate with degraded systems. Exercises must include and test these concepts of operation.

Milestone Decision Authority Roles and Responsibility

Clear roles and responsibilities of those with milestone decision authority are essential if a new acquisition process is to be successful and the desired outcomes achieved. The lack of clarity in this regard is one of the most significant impediments to successful implementation of the current process. The task force believes that the preferred approach should be delegation to the lowest level acquisition decision authority consistent with program risk.

Furthermore, acquisition authority and expertise within OSD is currently spread across several organizations—under the USD (AT&L), in OASD (NII)/DOD CIO, and in the Business Transformation Agency. At the Service level, similar disaggregation of responsibility also exists. This disaggregated approach seems inefficient, resulting in a lack of enterprise-wide architecture and coordination. Qualified IT acquisition and systems analysis and architecture personnel are scarce and should not be spread among separate OSD organizations. Given the speed with which information technology advances, this disaggregation exacerbates the ability to maintain currency and coordination within the acquisition workforce.

It is important to recognize that IT acquisition requirements are different and, because IT touches nearly everything acquired by the Defense Acquisition Executive (the USD (AT&L)), it is more than a side consideration. Bringing together the expertise from many organizations into a single one will help to ensure that the unique attributes of IT programs are better understood. In addition to the milestone decision authority responsibilities and organization, the Defense Acquisition Executive advisory staff (DDR&E, PA&E, OT&E, Comptroller) issue definition and resolution process often contributes to extended IT acquisition times.

RECOMMENDATION 3. ACQUISITION AUTHORITIES AND ORGANIZATION

The USD (AT&L) is responsible for all acquisitions, the acquisition workforce, and is the Milestone Decision Authority for all major defense acquisition programs, major automated information systems, and special interest programs. The USD (AT&L) should:

- aggressively delegate milestone decision authority commensurate with program risk
- consider a more effective management and oversight mechanism to ensure joint program stability and improved program outcomes

Consolidate all acquisition oversight of information technology under the USD (AT&L) by moving into that organization, those elements of the OASD (NII)/DOD CIO and Business Transformation Agency responsible for IT acquisition oversight. The remainder of OASD (NII)/DOD CIO is retained as it exists today, but should be strengthened as indicated in the previous recommendation.

Acquisition Expertise

A high degree of relevant technical and proven management capability is needed for IT system acquisition leadership. In addition, a set of IT domain experts are needed within the acquisition community to support acquisition oversight and decision-making. OSD and the Services need IT acquisition staff with extensive experience in large-scale, embedded, and commercial IT.

Today, the subject matter competencies required for successful enterprise IT system acquisition are too often missing in government managers responsible for program execution. Skills in program administration are confused with skills in operational process design and/or with skills in IT. Contracting, budgetary, and organizational design debates crowd out concepts of operations and system engineering debates. Further, architecture is too often viewed as a paper exercise rather than a model-driven, analytically supported, and rigorous engineering process incorporating enterprise-wide considerations for functionality and interface definition. Within the Department, IT expertise is scarce and the competition for talent is increasing.

There is no substitute for experienced program managers with track records of proven success. In a review of major IT acquisition programs where cost, schedule, or quality and performance were issues, three root causes emerged. First, senior leaders lacked experience and understanding. Second, the program executive officers and program managers had inadequate experience. Third, the acquisition process was bureaucratic and cumbersome, where many who are not accountable must say “yes” before authority to proceed is granted. Some of these issues have been discussed previously in this testimony, but among these problems, lack of experience dominated.

The experience and qualifications of OSD and Service leaders, and program executive officers and program managers is critical to making the **right judgments** to begin a program with executable objectives and then manage it to successful completion.

RECOMMENDATION 4. ACQUISITION EXPERTISE

The Secretary of Defense shall require that the defense acquisition executives have proven and relevant business experience in the appropriate areas of acquisition, product development, and management. Such qualifications apply to the ASD (NII)/DOD CIO and Service and agency CIOs as well.

The USD (AT&L) must work with Service and agency acquisition executives to improve the capabilities and selection process for program executive officers and program managers.

The USD (AT&L) shall direct the Defense Acquisition University (DAU), in coordination with the Information Resources Management College, to integrate the new acquisition model into their curriculum.

The DAU must staff with faculty knowledgeable and capable in contemporary product development management and acquisition practices versus individuals trained in only the old system.

Bottom Line Regarding IT Acquisition

The bottom line is that the inability to effectively acquire IT systems is critical to national security. Today the United States has the most capable fielded war fighting systems in the world. Information technology is critical to a wide range of capabilities: command and control, decision systems, precision weapons, and situation awareness. The task force found that performance of the Department's current IT acquisition process is not acceptable. Thus, the many challenges surrounding information technology must be addressed if DOD is to remain a military leader in the future.

For information technology, actions in the four areas discussed above—acquisition policies and process, roles and responsibilities of the CIO, milestone decision authority roles and responsibilities, and acquisition leadership expertise—will improve the acquisition of information technology in DOD. But caution is offered that emphasis and focus only on the acquisition process is not enough. While a new process is needed that better takes into consideration the unique aspects of information technology, process improvements alone will not yield success. If the

matters associated with responsibilities and authorities, organization, and expertise are not also addressed, the new process proposed here is likely to meet with the same outcomes as process improvements recommended by other groups who have studied this issue. This set of recommendations is designed to both streamline the IT acquisition process and address the fundamental problems that exist in the system today.

Overall Conclusion

Even if all the recommendations put forth in this testimony are implemented, it is recognized that unanticipated problems will arise during the course of any acquisition or product development managed by experienced and well intentioned people. The only way to minimize the unintended and potentially disastrous consequences of such problems is to quickly recognize and deal with them. If the culture is to use problems as a stick to punish people, then issues will not likely be brought to the forefront in a timely manner and the problems that follow will escalate. DOD acquisition programs are executed on an open stage—creating a difficult job for the best leaders. It is critical that all stakeholders align to deliver our best national security potential.

As has been mentioned, there is no “silver bullet” to fixing defense acquisition. But, in the view of the DSB, the Department can improve its acquisition processes—with the Secretary of Defense in the lead, supported by Congress. The Department must focus on four key areas:

- 1. Buying the right things**
- 2. Selecting an effective leadership team**
- 3. Reforming and streamlining the acquisition process**
- 4. Improving acquisition execution**

All of these elements are essential, none can achieve results alone. With a growing deficit, rising costs, and declining output, it really is not an option to let the status quo continue. Fixing acquisition is a national security issue. We do not want to find ourselves wringing our hands over the state of our national security because we chose not to act.



Ronald (Ron) Kerber

Dr. Ronald Kerber is an experienced executive with a successful record of leading and growing domestic and global businesses. His leadership responsibilities have included general management, innovation, product development, procurement, cost reduction, and profitability in diverse, global organizations. He currently splits his time among a variety of entrepreneurial and pro bono activities as president of SBDC, a small consulting firm; Partner and Cofounder of Dominion Development Company and Proffit Station LLC.; visiting professor at The Darden Business School, the University of Virginia; and member of the Department of Defense Science Board.

During ten years as executive vice president and chief technology officer at Whirlpool, Dr. Kerber had line responsibility for global product development and global procurement, and P&L responsibility for three global businesses: microwave ovens, air conditioners, and compressors. Prior to his tenure with Whirlpool, Kerber served as vice president of advanced technology and business development and a member of the Executive Committee at McDonnell Douglas; as deputy undersecretary of defense for research and advanced technology, DUSD(R&AT); and as a program manager at the Defense Advanced Research Projects Agency (DARPA) in the Department of Defense. Dr. Kerber was also a member of the technical staff of The Aerospace Corporation.

Before beginning his business career, Dr. Kerber was a professor of electrical and mechanical engineering and associate dean of engineering for graduate studies and research at Michigan State University. He is coauthor of *Strategic Product Creation*, McGraw Hill, 2007 and has published more than 60 technical articles. He is the recipient of the Secretary of Defense Medal for Outstanding Public Service, the Michigan State University Teacher Scholar Award, the Purdue University Distinguished Engineering Alumni, and Outstanding Aerospace Engineer Award. He was a NASA Fellow at the California Institute of Technology and is a Batten Fellow at The Darden Business School, the University of Virginia. Dr. Kerber is a member of the Board of Trustees of Anser Corporation.

Dr. Kerber received his B.S. degree from Purdue University, and M.S. and Ph.D. degrees in engineering science from the California Institute of Technology.

**DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION**

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(4), of the Rules of the U.S. House of Representatives for the 111th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Armed Services Committee in complying with the House rule.

Witness name: RONALD L. KERBER

Capacity in which appearing: (check one)

Individual

Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: _____

FISCAL YEAR 2009

federal grant(s)/ contracts	federal agency	dollar value	subject(s) of contract or grant

FISCAL YEAR 2008

federal grant(s)/ contracts	federal agency	dollar value	subject(s) of contract or grant

FISCAL YEAR 2007

Federal grant(s)/ contracts	federal agency	dollar value	subject(s) of contract or grant

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2009): _____;
 Fiscal year 2008: _____;
 Fiscal year 2007: _____.

Federal agencies with which federal contracts are held:

Current fiscal year (2009): _____;
 Fiscal year 2008: _____;
 Fiscal year 2007: _____.

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2009): _____;
 Fiscal year 2008: _____;
 Fiscal year 2007: _____.

Aggregate dollar value of federal contracts held:

Current fiscal year (2009): _____;
 Fiscal year 2008: _____;
 Fiscal year 2007: _____.

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2009): _____;
Fiscal year 2008: _____;
Fiscal year 2007: _____.

Federal agencies with which federal grants are held:

Current fiscal year (2009): _____;
Fiscal year 2008: _____;
Fiscal year 2007: _____.

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2009): _____;
Fiscal year 2008: _____;
Fiscal year 2007: _____.

Aggregate dollar value of federal grants held:

Current fiscal year (2009): _____;
Fiscal year 2008: _____;
Fiscal year 2007: _____.

**Disclosure Form Addendum
for
Ronald L. Kerber
Testifying, July 9, 2009**

I am testifying in my individual capacity and as a member of the Defense Science Board. I am not representing any other entity. As noted in my curriculum vitae, I do serve on the Board of Trustees of Analytic Services Inc., an independent, not-for-profit research institute that performs studies and analysis for the Department of Defense, Department of Homeland Security, the Intelligence Community, other federal agencies, and other public agencies and institutions.

*Ronald L. Kerber
July 6, 2009*

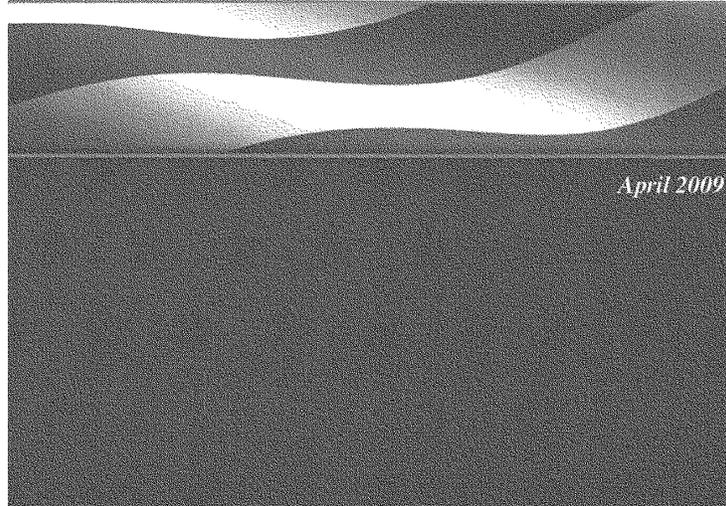
DOCUMENTS SUBMITTED FOR THE RECORD

JULY 9, 2009



Report of the
Defense Science Board

Creating a DOD Strategic Acquisition Platform



This report is a product of the Defense Science Board (DSB).

The DSB is a federal advisory committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report was prepared by the DSB Task Force on Future Perspectives; the task force completed its information gathering in March 2009.

This report is unclassified and cleared for public release.

Creating a DOD Strategic Acquisition Platform

FIXING THE DOD ACQUISITION PROCESS IS A CRITICAL NATIONAL SECURITY ISSUE—REQUIRING THE ATTENTION OF THE SECRETARY OF DEFENSE. ... THE INCOMING LEADERSHIP MUST ADDRESS THIS CONCERN AMONG ITS TOP PRIORITIES, AS THE NATION'S MILITARY PROWESS DEPENDS ON IT.

The United States must be prepared to respond to a broad set of national security missions, both at home and abroad—strategic deterrence, conventional and asymmetric warfare, and defense of the homeland are among the most prominent. Yet many deficiencies exist in defense capabilities needed to support these missions—systems are aging and technologies are becoming obsolete. Systems such as the B-52 bomber fleet, cruise missiles, tanker aircraft, the nuclear stockpile, and the strategic force are reaching the end of their service. Intelligence, surveillance, and reconnaissance systems are becoming less effective in the face of rapid advances in technology. The interoperability of communication systems continues to be a major concern on the battlefield.

A robust acquisition process is critical to sustain a strong arsenal of effective weapon systems. When hostilities in Iraq and Afghanistan draw to a close, it is realistic to anticipate reductions in the defense budget. At the same time, the Department of Defense (DOD) will need to refresh materiel depleted in those wars, while continuing the process of replacing aging systems—all of which increase the need for a more effective and efficient acquisition process. Capable adversaries who are adept at acquiring and adapting weapons from widely available commercial technology are yet another factor. These pressures are coming to bear at the same time many observers have recognized that the Department of Defense acquisition process has been broken for some time.

Fixing the DOD acquisition process is a critical national security issue—requiring the attention of the Secretary of Defense. DOD needs a strategic acquisition platform to guide the process of equipping its forces with the right materiel to support mission needs in an expeditious, cost-effective manner. The incoming leadership must address this concern among its top priorities, as the nation's military prowess depends on it.

This report offers recommendations for rebuilding the defense acquisition process, drawn from numerous reports over the past few years prepared by the Defense Science Board, an advisory body to the Secretary of Defense. We believe this report offers useful insight for the Secretary of Defense and his transition team to address critical acquisition challenges.



Contributors

Dr. Ronald Kerber, Chair

Dr. Craig Fields

Dr. Jacques Gansler

Dr. Robert Hermann

Dr. William Howard

Dr. Miriam John

Mr. Robert Lucky

Mr. Larry Lynn

Mr. Robert Nesbit

Mr. Vincent Vitto

Table of Contents

Fixing the acquisition process is a national security issue	1
Today, the defense acquisition process takes too long to produce weapons that are too expensive and often technically outdated by the time they are fielded.....	1
There have been many attempts to fix the acquisition process, but none, as of yet, have been successful.....	4
Buy the right things.....	8
Fixing acquisition begins with buying the right things to support national security objectives.....	8
Select an effective leadership team, with proven, relevant experience.....	13
The acquisition process cannot be fixed without proven, experienced leadership in the Office of the Secretary of Defense and the military services.....	13
Leadership also plays an important role in ensuring that program and process owners and stakeholders are aligned with common goals.....	15
Reform and streamline the acquisition process.....	17
The current state of the acquisition process is unacceptable and in desperate need of reform.....	17
Improve acquisition execution	31
Acquisition improvements are not enabled by policy and process reforms alone. Those changes lay the framework for success, but must be coupled with efficient, effective execution led by experienced leaders.....	31
Urgent action is needed.....	38
Congress can and must be part of the solution.....	38
References	40

Fixing the acquisition process is a national security issue

Today, the defense acquisition process takes too long to produce weapons that are too expensive and often technically outdated by the time they are fielded.

Typical major system acquisitions take 10 to 15 years, while new product development in the commercial sector of similarly complex systems takes one-third to one-half of that time. Acquisition of information technology, on which many defense systems are critically dependent, also exceeds typical commercial development time—taking three to four times as long. These development times are far outpaced by the rapid advances in technology, which means that subsystem technology can be one or two generations old by the time a system is provided to war fighters in the field—unless upgrades are incorporated before the system is fielded. Furthermore, programs often have large cost overruns, long schedule delays, and unsatisfactory product quality and performance.

At the same time, the nation faces very adaptive adversaries. The United States is no longer in a unique position of technological supremacy. Many types of advanced technology are readily available on the world market. Adversaries are becoming very adept at fashioning new weapon capabilities from commercially available technology—"good enough" systems are developed and fielded quickly. And, they are often far more agile in doing so than the United States. Most military planners recognize that a robust military strategy combines a formidable offense with a capable and comprehensive defense. But some current adversaries can target U.S. vulnerabilities and time their attack without concern for the risk of U.S. offensive retaliation—as they have little of value to put at risk. Adaptive adversaries are able to identify U.S. vulnerabilities and create effective systems to exploit them—one example is improvised explosive devices that became prominent early in the Iraq conflict and continue to plague U.S. forces. When rogue states

and terrorists employ this strategy, it creates a critical challenge for the nation. Thus, we must enhance our ability to rapidly and effectively transition commercial and military-unique products to our war fighters in the field.

While this scenario applies to all weapon systems, information technology presents a somewhat different set of challenges due largely to the fact that it is an important enabler for so many defense capabilities. It underlies the nation's ability to gain better intelligence, better situational awareness of the battlefield, better communications, and more precision in weapon system delivery. In fact, the use of information technology is pervasive, from administrative systems for managing business processes, to embedded subsystems in major weapon systems—comprising as much as 90 percent of the cost of some new systems.

Despite its crucial importance, the Department's ability to acquire information technology is fraught with problems. Driven by the short half-life of commercial information technology, hardware supportability, software applications, and evolving operational requirements, the need for continuous upgrades and product improvement is a reality that must be accommodated by the acquisition process. In addition, it is often difficult to technically validate these programs to ensure that what is being delivered is in fact what is expected, raising the potential for unknown system vulnerabilities.

Furthermore, many information technology systems are managed as joint programs, ultimately used by more than one of the military services. Systems such as intelligence, surveillance and reconnaissance; command and control; and communication systems are often acquired as joint programs to ensure interoperability and common fielding dates among the user services. As a result, managing these programs requires joint cooperation among the services—an endeavor that often poses a challenge to effective acquisition. Additionally, achieving and maintaining stable budgets and system interoperability—systems developed to operate with many others on the battlefield—remain important issues.

**PREVIOUS EFFORTS
AT ACQUISITION
REFORM HAVE
FAILED TO ADDRESS
THE ROOT CAUSES
OF THE PROBLEM,
FOCUSING INSTEAD
ON RE-ENGINEERING
THE MECHANICS OF
THE ACQUISITION
DECISION PROCESS.**

Finally, the acquisition of services receives far less attention than that of materiel, yet it is a growing part of the defense budget—representing about 50 percent of the acquisition budget, which totaled nearly \$400 billion in fiscal year 2008.¹ Services range from support to the battlefield, to airlift and logistics, to security services, janitorial services, and studies and analysis. Such activities are not only necessary, but also advantageous to contract as services so that DOD personnel can devote their time to the jobs they were trained to do. Yet it is still reasonable to ask whether all such contracts are necessary and whether they could be contracted more efficiently. Service contracts should be subjected to scrutiny and be required to meet certain criteria similar to materiel acquisition.

The problems of acquisition execution outlined above have been well known for years. Yet an even more important deficiency is the process of determining what to buy. The strategic plan for acquiring military capabilities is only loosely aligned with national security objectives and the military missions to achieve them. The military services are tasked to train and equip the nation's forces and they often control the input into the process—defining the capabilities to be acquired. The combatant commanders, who actually use forces and equipment in the field to execute missions, have little input in determining which next-generation capabilities to acquire. Often, present programs reflect past missions and seldom adequately support joint needs, despite the fact that ongoing combat experiences demonstrate new joint needs and interoperability issues. Clearly the driving agenda item the Department needs to address is improving the process of evaluating and deciding what to buy to support the highest priority national security mission needs.

The shortcomings addressed here point to an acquisition process that is not adequately meeting the needs of the Department of Defense. Fixing this process must become a departmental priority—led by the Secretary of Defense.

1. Data derived from the Federal Procurement Data System—Next Generation (FPDS-NG); <https://www.fpds.gov> [March 2009].

There have been many attempts to fix the acquisition process, but none, as of yet, have been successful.

The defense acquisition process has been studied for decades—by the Packard Commission, the Government Accountability Office, the Defense Science Board, think tanks, commissions, and many other organizations, including the Department itself. For decades, these studies have identified numerous flaws—problems with bureaucracy, accountability, overlap of authority, inefficient processes, and inexperienced leadership. And over the years, the Department has made a series of attempts to “fix” acquisition—usually at the direction of the Under Secretary of Defense for Acquisition, Technology, and Logistics. Yet problems persist—major system acquisitions still take too long, costs are overrun, and concerns remain over product performance and quality.

Why have previous efforts so often failed? In part, it is because they fail to address the root causes of the problem, focusing instead on re-engineering the mechanics of the acquisition decision process. Many problems appear to be caused by the use of immature technology, requirements “creep,” or funding instability. Such problems, however, are really *only symptoms* of the lack of experienced judgment on the part of Department personnel who structure acquisition programs in a way that will almost certainly lead to failure.

Moreover, many organizations in DOD are often not aligned with departmental acquisition goals and objectives. The staff of the Office of the Secretary of Defense (OSD)—including the Director, Program Analysis and Evaluation; the Comptroller; the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer; Director, Defense Research and Engineering; and Director, Operational Test and Evaluation—the military services, and the Joint Staff are all power centers that not only often fail to be aligned with each other, but sometimes are not even aligned within themselves. Many of the

**FIXING ACQUISITION
IS A CHALLENGE
BIGGER AND
BROADER THAN
THE SCOPE OF THE
ACQUISITION UNDER
SECRETARY—THE
SECRETARY OF
DEFENSE MUST LEAD
THE CHARGE ... IT
SHOULD BE AMONG
HIS TOP PRIORITIES.**

Secretary's advisory staff, who are not accountable to deliver acquisitions, can also stall a program's ability to proceed through the process while awaiting their input.

Perhaps the most important reason that previous efforts have failed, however, is that the problem has been left to the Under Secretary of Defense for Acquisition, Technology, and Logistics. Effective acquisition is a challenge that is much bigger and broader than the authority or scope of power of that office. Many of the organizations, functions, and processes that support acquisition are not, and should not be, the responsibility of the acquisition under secretary. Fixing defense acquisition is a challenge that can only be successfully addressed by the Secretary of Defense and it should be among his top priorities. The Secretary not only must lead the charge within DOD to fix the acquisition process, but also must inform the Congress of departmental actions and enlist its support for his agenda, lest Congress act independently in a way that undermines his efforts.

There is no silver bullet for "fixing" acquisition. As noted previously, many studies have identified many problems and offered many solutions. One particular difference in the findings and recommendations discussed in this report, drawn from a decade of past studies by the Defense Science Board, is in how the problem is defined. Fixing acquisition challenges must begin with leadership action by the Secretary of Defense. A plan to address acquisition processes should focus not only on "how" the Department buys material, but also "what" materiel the Department buys, who is involved in the process, and whether support systems help or hinder.

The Secretary of Defense must create a strategic acquisition management platform comprised of four critical elements.

1. Buy the right things.

The strategic military planning system, DOD's regime for deciding "what to buy," has a weak analytic foundation. When we buy the wrong thing, we blame the acquisition system. But that system is responsible for "how to buy."

Before fixing acquisition processes, the Secretary must reform the strategic military planning system and create a genuine “business plan” for DOD. This resource-balanced plan should be developed with greater involvement of the regional combatant commands and better use of systems engineering, and modeling and simulation.

2. Select an effective leadership team.

Proven, relevant experience is needed in the Office of the Secretary of Defense, the military departments, and defense agencies. Today, many people are inexperienced, from leadership to program managers. Few have a personal track record of repeated successes at acquisition. Trial-and-error and on-the-job training can be really expensive. The Department needs to hire and assign individuals with proven records of acquisition success. At the program level, this may mean facing the possibility of not doing a program until the right people are available.

3. Reform and streamline the acquisition process.

A single acquisition process cannot meet the demands of acquiring major systems, commercial derivatives, and information technology systems, as well as rapidly fielding critical war fighting needs, especially in a time of crisis. The process of buying major systems, information technology systems, and commercial derivatives needs to be streamlined with strong, up-front systems engineering support. The case of information technology presents unique challenges—in stand-alone systems, embedded systems, and net-centric infrastructure. A new decision process is needed that recognizes the rapid advances in information technology and plans for frequent and efficient upgrades after delivery. The ability to field critical war fighting needs also requires a new approach—a standing acquisition capability that can fulfill these requirements in a timely way, as there is little doubt that the need will continue.

4. Improve acquisition execution.

Acquisition improvements are not enabled by policy and process reforms alone. They must be coupled with efficient, effective execution. Key areas where improvement in management and execution are needed include: product development, contract award and management, acquisition workforce, acquisition integrity, and process metrics. Central to these improvements is experienced personnel—in leadership, in the acquisition workforce, and, equally important, in the contractor base. Up-front attention to systems engineering during product development, as well as keen attention to acquisition integrity, are also essential.

Many may say that they are already doing what we recommend. In fact, the recommendations of this report are essentially common sense and one may find each concept used in an isolated case. The real message is that a comprehensive approach must be used uniformly across the defense enterprise to be successful. If “they were already doing this” comprehensively there would not be problems with defense acquisition or need for this report.

As has been mentioned, there is no “silver bullet” to fixing defense acquisition. But, in the view of the Defense Science Board, the Department can improve its acquisition processes—with the Secretary of Defense in the lead, supported by Congress, and focused on each of these essential four areas, none of which can achieve results alone. With a growing deficit, rising costs, and declining output, it is not an option to let the status quo continue. Fixing acquisition is a national security issue. We do not want to find ourselves wringing our hands over the state of our national security because we chose not to act.



Buy the right things

**FIXING
ACQUISITION
BEGINS BY
SELECTING THE
RIGHT THINGS
TO ACQUIRE TO
SUPPORT
NATIONAL
SECURITY
OBJECTIVES.**

Fixing acquisition begins with buying the right things to support national security objectives.

Fixing the acquisition system—“how to buy”—is dependent on fixing the strategic military planning system—which includes decisions on “what to buy.” When we buy the wrong things, we blame the acquisition system, when the problem lies with the strategic planning system. The Department’s regime for deciding what to buy has a weak analytic foundation and must be reformed.

The Department of Defense has a large formal process, the Quadrennial Defense Review, to establish national security objectives and the strategic direction and missions to support them. It is common knowledge, however, that recent reviews have had little impact on changing the acquisition agenda of the military services. In such a forum, the Services tend to “protect” their current agenda and programs, while new or different acquisition alternatives or programs to meet urgent needs have difficulty surviving.

The operational leaders—the combatant commanders—are not effectively represented in these processes. Since these commands are where the products of acquisition come together as an integrated force, they should be more involved in the issues of aligning what is to be acquired to the strategies of their mission responsibilities and the ability of these systems to operate together. While, currently, they often bring more tactically-oriented needs to the table, they should be tasked to play a larger role in the development of longer-term strategies for meeting their responsibilities, in order to lay a stronger analytic foundation for acquisition decisions.

The commands also bring a sense of urgency and reflect the need for systems that can effectively operate with others on the battlefield—commonly referred to as

interoperability. For decades we have fielded systems that lack needed interoperability and do not adequately support joint intelligence, surveillance, and reconnaissance and munitions needs; and we have struggled with less than acceptable communication systems. Instead, major platforms tend to remain at center stage of the acquisition agenda. The consequences include soldiers resorting to using cell phones to communicate in war zones in Iraq and Afghanistan, among other issues.

The Department should define critical capability needs to support each mission. Today, "requirements" are used to define capability needs, implying that nothing less than a specified set of criteria is sufficient. Instead, a more prudent answer is to buy the best capability affordable, in the quantity desired, and fielded in as timely a manner as possible. Such a strategy does not preclude development of revolutionary systems like stealth aircraft, but it does encourage incremental spiral development and system block upgrades to improve the timing of fielded capability while lowering the overall risk.

To identify the specific capability, a clear analysis of alternatives and a comprehensive systems engineering analysis are required—including man-in-the-loop simulations to test system effectiveness and trade-offs. Such an approach results in a clearer understanding of the value of performance characteristics, the costs and benefits of various features, and a time-to-field that is based on a thorough assessment of technology development needs. It is important to note that neither intuition nor experience alone will suffice. It is also essential to determine what can be accomplished through innovation to avoid the common pitfall of "preparing for the last war" rather than looking to the future.

With the type of analytic underpinnings described here, informed decisions on "requirements" can be made in light of effectiveness, cost, quantity to buy, and time-to-field. And a realistic acquisition schedule can be developed. This understanding serves as a useful basis to program

AT PRESENT, THERE IS NO PLAN IN DOD THAT QUALIFIES AS A BUSINESS PLAN ... SUCH A PLAN REQUIRES GREATER INVOLVEMENT OF THE REGIONAL COMBATANT COMMANDS AND A STRONG ANALYTIC FOUNDATION.

managers as they inevitably deal with unforeseen problems that will arise and require additional trade-off decisions during the course of the acquisition process. Program managers ultimately need the authority and knowledge to manage such trade-offs and to prevent requirements from growing inappropriately. They must also have the support of departmental leadership.

How can the Department reorient its decision-making processes to ensure that it buys the right things?

The most important action that the Secretary of Defense can take is to reform the strategic military planning system and establish a genuine business plan for DOD to discipline resource allocation in support of national security objectives. The plan must be comprehensive in identifying the objectives of the Department and the human and financial resources needed to accomplish them. Developing this plan requires greater involvement of the regional combatant commands and a strong analytic foundation through better use of systems engineering and modeling and simulation.

This resource-balanced plan must by necessity include an outline of what to buy in light of the nation's security priorities, and ensure that each program is fully funded from acquisition to sustainment. Specifically, this means including in the plan materiel acquisition objectives, planned fielding dates, and the resources necessary to acquire and insert them effectively into the field. In other words, the plan must relate resources to mission purpose. In effect, such a plan will discipline the resource allocation and acquisition processes and will give decision makers a clear understanding of the need for, and impact of, resource decisions. At present, there is no plan in DOD that qualifies as a business plan.

The elements of the business plan should clearly define military missions needed to support national security objectives and outline how the Department will accomplish these objectives—what materiel to buy, how it should be supported, when it should be

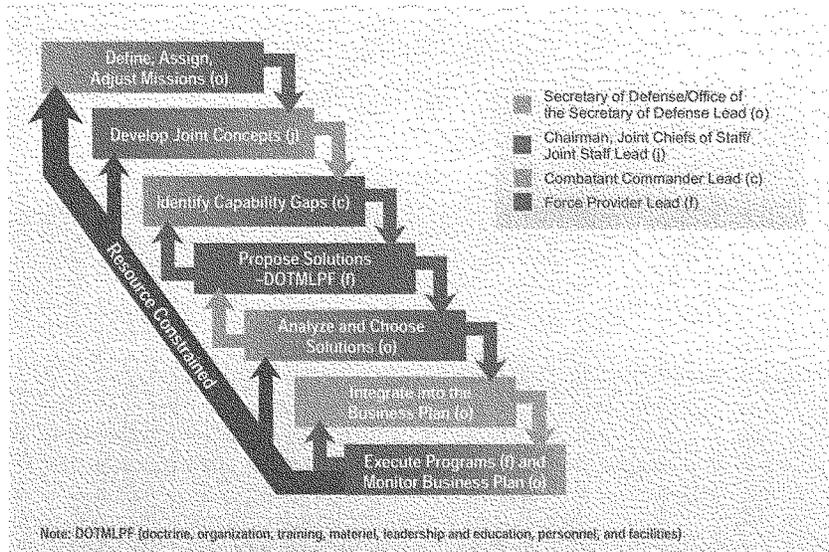
operational in the field, and what forces to train and prepare. The plan should also identify who will be responsible for execution of each element of the plan as well as the allocated resources. It is necessary for the plan to be enforced to ensure accountability. This plan is intended to be a high-level document, typically not more than 40 to 50 pages in length.

To create and execute such a plan requires involvement of key decision makers in the Office of the Secretary of Defense, the Joint Staff, and the military departments, beginning with the Secretary of Defense. Key steps in the process are as follows:

- ❑ The Secretary of Defense, supported by the Chairman, Joint Chiefs of Staff, defines, assigns, and adjusts the priority missions in support of the national security strategy.
- ❑ The Chairman leads the process to develop joint concepts, with strong participation from the combatant commanders.
- ❑ The combatant commanders identify needed capabilities, with support from the Joint Staff, and active involvement from the force providers.
- ❑ The Secretary of Defense, with support from the Chairman, the Joint Staff, and the force providers chooses solutions. The Secretary and staff integrate the solutions into the business plan, specifying what is to be done, in what time period, with what resources, and what output.
- ❑ Force providers are then fully accountable for delivering the capability on time and within allocated resources, while the Secretary's staff monitors the overall process.

An important aspect of the process is feedback. Earlier steps are informed by experience throughout the process in a continuous cycle of change within resource constraints. The business plan provides discipline for the system—the single roadmap that all players in the process must follow.

A business plan will help to ensure better management and accountability of programs that cross individual service lines. Joint programs, such as intelligence, surveillance, and reconnaissance systems and communications capabilities, are critical to mission success. But these programs are typically not well managed in the acquisition process. The military services tend to give them low priority relative to their "own" programs that tend to be more platform-oriented. With a business plan that identifies what to buy and who is responsible, and ensures funding, appropriate priority will be given to all programs--joint and service specific.



Creating and executing a multi-year business plan would involve key decision makers within the Department. It would enforce accountability and provide a clear understanding of the need for, and impact of, resource decisions.

Select an effective leadership team, with proven, relevant experience

PEOPLE ARE
INEXPERIENCED,
FROM THE
LEADERSHIP
TO PROGRAM
MANAGERS,
VIRTUALLY
NOBODY HAS
A PERSONAL
TRACK RECORD
OF REPEATED
SUCCESS AT
ACQUISITION.

The acquisition process cannot be fixed without proven, experienced leadership in the Office of the Secretary of Defense and the military services.

People are inexperienced. From the leadership to program managers, virtually nobody has a personal track record of repeated success at acquisition. Trial-and-error and on-the-job learning can be really expensive.

The Packard Commission made this point clear when recommending that the acquisition leadership have "a solid industrial background." Yet the Commission's intent is often ignored when the rules are stretched so that the acquisition executives in OSD and the services are appointed with little or no proven, relevant, or successful business experience. Without relevant experience to guide decision-making, these leaders often rely on the bureaucracy to make decisions for them.

Lack of seasoned leadership is part of the many problems plaguing current acquisition programs. Leadership shortcomings result in programs that are not structured for successful execution due to a plethora of difficulties:

- lack of sufficient up-front analysis of alternatives
- poor systems engineering support
- inadequate performance, cost, and value trade-offs
- poorly designed product development strategies
- poor management of technical risk
- growing requirements
- selection of inexperienced contractors
- poor contract incentives
- budget instability

**THE DEPARTMENT
MUST HIRE
AND ASSIGN
INDIVIDUALS WITH
PROVEN RECORDS
OF ACQUISITION
SUCCESS.**

Since people tend to debate what they understand, contracting, budgetary, and organization design debates crowd out those involving product development management issues, technical and production challenges, concepts of operations, and systems engineering. Skills in program administration are often confused with skills in acquisition management ability.

Solving these problems begins with selecting the right leaders who can make decisions based on judgment gained through experience. It also requires proper incentives—elements essential for success. Incentives can be both positive and negative—from recognition of outstanding performance to public visibility of inadequate performance. Today's leaders require a combination of business, technical, and human resource management capability. Our nation can afford nothing less than the best, experienced people for these critical acquisition positions.

Along with experienced leaders, the civilian and military workforce must be upgraded as well. The first step is to select managers of major systems programs—that is, program executive officers and program managers—that have demonstrated successful performance in managing programs of increasing complexity. Program success is more likely, even if a program is delayed, if the right leadership can be put in place from the start so that the program initiates with goals and objectives that can be realized. The "best available" may not be good enough. It is up to the acquisition under secretary to establish such guidelines and ensure that they are followed.

The Department must hire and assign individuals with proven records of acquisition success—even facing the possibility of not doing a program if the right people are not available.

The Secretary of Defense should issue guidance that top acquisition appointments be filled with individuals who have proven, successful, and relevant commercial experience.

The Under Secretary of Defense for Acquisition, Technology, and Logistics should require that program executive officers and program managers have

demonstrated successful performance in managing programs of increasing complexity before appointments are made to lead major systems programs.

Leadership also plays an important role in ensuring that program and process owners and stakeholders are aligned with common goals.

The personal interests of many individuals involved in the acquisition process do not always align with the interests of the nation. It is in the self interest of too many people not to fix the acquisition system: they are financially rewarded and their career is sustained by keeping things as they are.

Major programs experience delays and interruptions because senior department leaders—in the Office of the Secretary of Defense, the military services, and the Joint Staff—are not aligned with common goals. It is not unusual for the lead times for major program reviews to extend for months because of problems identified late in the game or brought forward in an untimely manner by various organizations in the Department.

The input of acquisition advisors—Director, Program Analysis and Evaluation; Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer; Director, Defense Research and Engineering; Director, Operational Test and Evaluation; the Comptroller, and others—is valuable to the acquisition process. Their insight can lead to more successful program outputs. But it must be provided in a timely manner—starting at program initiation and continuing throughout program execution. It should be viewed as a failure of these offices if the first identification of a problem is at a major program review. This observation is not to be taken as a wish to suppress problems or issues. Rather, as a need to identify problems as soon as they are evident and work as a team to eliminate them.

Further, it is often the case in the military departments for the technical authority, which oversees standards and military certification, to operate outside the

**THE PERSONAL
INTERESTS OF
MANY INDIVIDUALS
INVOLVED IN THE
ACQUISITION
PROCESS DO NOT
ALWAYS ALIGN WITH
THE INTERESTS
OF THE NATION ...
THE SECRETARY
OF DEFENSE MUST
CREATE INCENTIVES
TO ALIGN ALL
STAKEHOLDERS
BEHIND COMMON
GOALS.**

programmatic chain of command—dependent from program management and systems engineering. A common entity supervising both the technical authority and program management often exists only at the highest levels. This means that those responsible for technical authority have no organizational responsibility for meeting cost and schedule requirements. Yet their input can have a significant impact on program decisions, and in turn program schedule and cost.

An inflexible and potentially adversarial separation of these two functions can often hamper useful program trade-offs, even in programs where such trade-offs were intended at program initiation. Instead, all those involved in the acquisition process—whether technical authority or program management—must be aligned along a common goal of achieving successful, timely program execution. After all, it is the war fighter who is ultimately affected when needed capabilities are not fielded in a timely manner—with the ultimate cost being needless loss of life.

The Secretary of Defense must take action to discipline the program review and execution process so that programs can proceed according to planned schedules. Program managers should not have to wait for stakeholder input before proceeding to program milestones—it should be provided throughout the acquisition process so that identified problems can be resolved long before major decision points arise. Once options are reviewed and due process of the various stakeholders has been considered, the Secretary must ensure that department leadership supports the decision and works as a cohesive team to achieve the desired goals. This means developing meaningful incentives for positive performance, including rewards and recognition. And, when necessary, levy appropriate discipline to those who defy Department decisions or try to game the system.

The Secretary should direct all leaders in the Office of the Secretary of Defense, the military services, and the Joint Staff, to align behind acquisition decisions and support program execution in a timely manner. The Secretary should follow through with scheduled periodic reviews of actual program performance, and should reward and discipline staff accordingly.

Reform and streamline the acquisition process

STREAMLINING MEANS FEWER BUT MORE EXPERIENCED PEOPLE, FEWER COMMITTEES, FEWER REVIEWS, AND MORE EFFECTIVE AND EXPERIENCED LEADERSHIP—WHICH SHOULD LEAD TO MORE EFFICIENT EXECUTION WITH LESS RISK.

The current state of the acquisition process is unacceptable and in desperate need of reform.

It is critical that the Department guide its acquisition decisions with a business plan that supports the nation's security objectives. But once a needed capability is identified under that plan, it is also critical that it be acquired within a streamlined decision process that can ensure timely, effective execution.

As discussed at the outset of this report, programs today take too long to procure and are often fielded with last-generation technology. Many programs have large cost overruns and deliver performance and quality that are less than desired. But even without cost overruns, programs are often approved without adequate funding, which creates serious execution problems throughout program acquisition.

Moreover, the current acquisition process must be disciplined with an infusion of effective leadership. Milestone decision reviews should take a few days of preparation, not the months and months currently required, which detracts from the real work of system development and acquisition. Streamlining is necessary to allow for fewer but more experienced people, fewer committees, fewer reviews, and more effective and experienced leadership. It would also lead to more efficient execution with less risk. By engaging stakeholders early and frequently during the acquisition process, more efficient decision reviews could be achieved.

The Secretary of Defense should task the Under Secretary of Defense for Acquisition, Technology, and Logistics to establish more streamlined acquisition processes.

While many disparate processes are not desirable, today's single acquisition process—geared toward major system acquisitions with significant technology development—is not effective at meeting the wide range of acquisition needs the Department must satisfy. These needs include major systems, commercial derivatives, information technology, and rapid fielding of new or adapted capabilities. Thus, tailored processes that take into consideration the unique attributes of these major classes of systems are needed.

The major system acquisition process needs to be infused with more in-depth systems analysis during the early stages of the process and planned using the tenets of spiral development and block upgrades, to the degree possible.

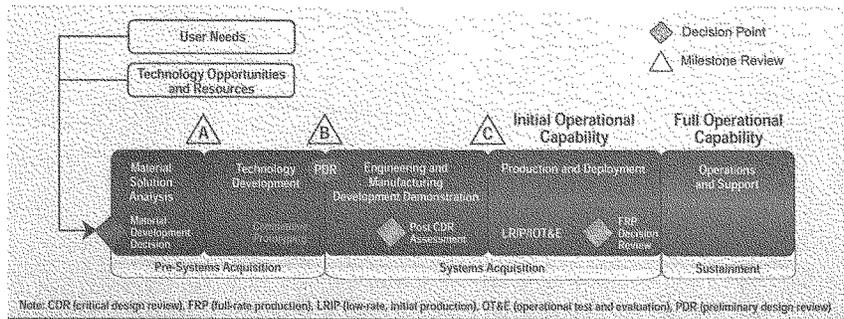
More thorough analysis is needed at the outset of system development and during key aspects of the development process, to include system and subsystem prototyping. Along with more in-depth and disciplined analysis, the acquisition plan should include an outline for acquiring new capabilities in multiple, shorter-phased increments—referred to as block upgrade acquisition made possible by incremental spiral development. An initial, base capability, that is operationally useful to the war fighter, is fielded and then enhanced in subsequent blocks until the full capability objectives are reached. As each increment is acquired, operational experience and experimentation will provide invaluable insights into what is needed and achievable in subsequent increments. It is recognized that each fielding must be accompanied by adequate training. Therefore a judicious balance must be made between fielding increments and the ability to train new capability without adding chaos in the field.

The goal of this approach is to dramatically reduce the time between identifying a new operational need and fielding operationally useful equipment. It helps to moderate risk by providing a steady stream of increased military capability that can be delivered on time and within budget. In contrast, the tendency today is toward giant single steps with high cost, schedule, and performance risk.

The Department of Defense has recently revised the acquisition decision process for major systems, codified in DOD Instruction 5000.02. One of the significant enhancements of the revised process is greater emphasis on system engineering and analysis in the early stages—the period where trade-offs can still be efficiently made based on the maturity of technology development and input from the war fighter as early increments of capability are released.

Key elements of the revised major system acquisition process are as follows:

- Begin the process with a critical analysis of alternatives prior to any decision milestones. Continue throughout the program with systems engineering and program analysis of alternatives to inform program manager decision-making. An effective analysis process will help properly evaluated program cost and schedule become recognized objectives during execution, along with performance. This approach is not feasible if the strict use of the “requirements” concept is followed. Replacing requirements with “capability needs” allows a meaningful trade-off to be made between performance, cost, and date-to-field.



The revised acquisition decision process for major systems places greater emphasis on system engineering and analysis in the early stages to allow input from the war fighter and trade-offs based on the status of technology development.

**UPFRONT ANALYSIS
AND PROTOTYPING
ARE CRITICAL
INGREDIENTS FOR
PROGRAM SUCCESS.**

- ☛ All acquisition programs should begin at a common entry point, with a materiel development decision—the mandatory start of the process. Programs should no longer enter in the middle of the process. Programs should not require or permit traditional technology development to be schedule-controlling events.
- ☛ Prototyping should begin during the technology development phase, and should be inserted whenever useful during the development process. Competitive prototyping is useful for initial contractor down selection. For systems that are likely to be procured over decades, such as fighter aircraft, prototyping of technology demonstrators should be used continuously to prepare for system renewal and as a test bed for emerging capabilities.
- ☛ A preliminary design review should be conducted before a commitment to final engineering design and manufacturing development is made. As part of this review, technology and production readiness should be assured.
- ☛ Program managers should consider using a configuration steering board to oversee system capabilities in order to minimize the tendency for desired capabilities to grow during the acquisition process—thus disciplining the system to incremental block upgrades.

These process changes should significantly improve the quality of product delivered through the defense acquisition process, contain costs, and dramatically shorten delivery times for major systems, by as much as one half. But to be successful, they must be accompanied by the effective leadership discussed previously in this report—as process changes alone, without experienced judgment, will have little impact.

Buying commercial or commercially derived systems (either domestic or foreign) presents a significant opportunity for the Department of Defense.

The globalization of technology and production means that defense-funded programs no longer drive technology development in many areas, and in fact,

**ACQUISITION OF
COMMERCIAL
PRODUCTS
REQUIRES A
DIFFERENT
MINDSET AND
MANAGEMENT
APPROACH.**

commercial technology now leads DOD in many areas. As a result, many advanced capabilities are available on the commercial market and offer an important option for supplying U.S. forces. While a military system designed from the bottom up can deliver a total solution to an identified capability, the goal of commercial or commercially derived systems is to acquire an “80 percent” solution that can be fielded rapidly and at a much lower cost and risk. The challenge is to successfully reap these advantages without the pitfalls typically experienced—challenges such as modifying the system to the extent that it no longer offers the advantage of buying commercially, inflexible procurement processes, or imposing military specifications without supporting systems engineering and analysis.

Acquiring commercial products requires a different mindset and a different management approach. Many acquisitions, such as the Littoral Combat Ship and the Presidential Helicopter Replacement, have faltered. Troubled programs appear to have a common failure paradigm—the failure to establish a clear understanding of program objectives that are well communicated at the outset, so that all involved, including DOD and contractor personnel, are working toward a common objective.

Further, many DOD organizations exist to maintain and support “military standards” and, thus, have technical authority over procurement standards. While such standards are appropriate for guiding the design and development of new DOD systems to be used in hostile combat environments, they are not always appropriate for procurement of commercial or commercially derived systems. In the case of commercial systems, cost, time to fielding, and other considerations may outweigh the need to infuse many or all military specifications and standards. Such trade-offs need to be made early and established clearly in program objectives.

Lack of experience in working with commercial products is another challenge. Problems arise when traditional DOD integrators, acting as prime contractors, have little experience with the particular commercial products they have contracted to

deliver by sourcing through a subcontract from a commercial vendor. In addition, problems arise when commercial products are modified to the point where they are more “custom” than “commercial.”

Buying foreign systems is another option that needs clarification in the acquisition process. Problems are similar to buying domestic commercial systems and the needed guidance is similar. Many government requirements (such as the Berry Amendment, Naval Vessel Rules, International Traffic in Arms Regulations, and others) directly contradict today’s design and manufacturing trends. The current rules significantly harm national security options by limiting DOD access to commercial and global technologies and allies’ markets. All of these factors must be considered or revised when buying commercial or commercially derived systems, whether domestic or foreign.

Importantly, DOD’s desire to acquire commercial systems should not be based on a presumption that commercial suppliers are interested in doing business with the Department. In fact, the onerous nature of government rules and requirements act as a deterrent to many potential suppliers. DOD needs to put incentives in place to encourage commercial and foreign suppliers.

The Under Secretary of Defense for Acquisition, Technology, and Logistics needs to clarify the objectives and process for acquiring commercial derivatives. The major systems acquisition process, with a modified technology development phase, is appropriate to support commercial product acquisition.

Acquiring information technology requires a different approach from major system acquisition—one that recognizes the unique attributes of information technology development and integration.

More and more of what DOD acquires is information technology (IT)—stand-alone systems, embedded systems, net-centric infrastructure, and business systems. We are at the fundamental limits of what we can do when acquiring IT: fundamental human limits in precisely and accurately specifying what is needed;

**CONTINUOUS
CHANGES AND
UPGRADES IN
INFORMATION
TECHNOLOGY ARE
A FACT OF LIFE
THAT MUST BE
ACCOMMODATED ...
A NEW ACQUISITION
PROCESS IS NEEDED
THAT ALLOWS FOR
RAPID ADVANCES IN
TECHNOLOGY, AND
FREQUENT AND
SWIFT UPGRADES
AFTER DELIVERY.**

fundamental technological limits in verifying that what we specify is actually delivered. In partial remedy, our acquisition system needs to enable swift and repeated upgrades in our IT systems, which is also needed to keep up with the ever changing improvement in technology.

Spending on information technology is rapidly growing in both embedded and stand-alone systems. IT system acquisition and IT upgrades to existing weapon systems represent a significant and growing percentage (up to 90 percent) of some current acquisitions. These acquisitions are taking longer and longer and the current process is too slow to keep up with advances in commercial technology to the point that fielded systems can be delivered with one- or two-generation old technology if there are no upgrades during the acquisition process. Furthermore, many current programs are exceeding cost and schedule baselines.

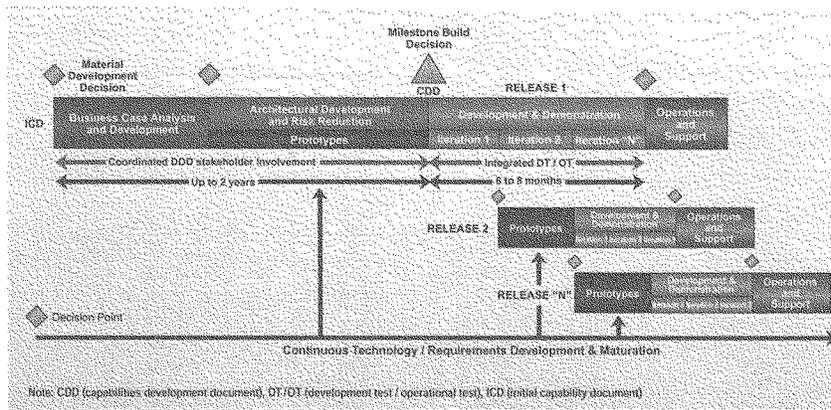
Continuous changes and upgrades in information technology are a fact of life that must be accommodated in the DOD acquisition process—a reality driven by the short half-life of commercial information technology, hardware supportability, software applications, and operational requirements. It is also hard to technically validate the capability delivered in IT systems—a factor that should be considered in the acquisition process to mitigate the addition of unknown vulnerabilities. In addition, many IT systems also reflect joint requirements, where resource stability and system interoperability issues remain.

The Under Secretary of Defense for Acquisition, Technology, and Logistics should adopt a new acquisition process for information technology.

A streamlined process for acquiring information technology would help to ameliorate many of the challenges faced in the acquisition of current systems and reflect the unique considerations described above. A key difference, from major system acquisition, is the level of technology development and system integration that is required. The major system acquisition process is required when there are substantial design trade-offs in both hardware and software and significant levels of technology development—the potential need for

advances in science or engineering must be considered when making trade-off decisions. In the information technology community, the term technology development often refers to the development of new software or integration of both hardware and software systems, and has little to do with advances in science or engineering.

Given these characteristics of information technology, the use of a new IT acquisition process is appropriate for purchasing new or replacement stand-alone IT systems and subsystems. The new process should also be used for upgrading IT systems embedded in existing weapon systems when there is little or no change in the hardware not associated with IT.



An acquisition process that accounts for the unique attributes of information technology would help to ameliorate many of the challenges faced in the acquisition of such systems today—enabling more rapid fielding of capabilities with latest-generation technology.

Key attributes of the new process are as follows:

- early and continual involvement of the user supported by system engineering design and performance value trade-offs
- multiple, rapidly executed increments/releases of capability
 - well-defined capability objectives, but not over-defined requirements for the initial increment
 - evolving capabilities for subsequent increments/releases
 - mature technologies (often with short half-life that require periodic refresh)
- early, successive prototyping to support an evolutionary approach combined with informal user trials
- early operational release of capability from within an increment
- modular, open-systems approach—designed for ease of updates
- available full funding of initial increment(s); solid funding stream for next overlapping upgrade increment(s)
- making schedule the priority for releasing available capability and not requiring (or expecting) a “yes” vote from every functional organization prior to decision milestones
- making sure that users are trained and prepared to receive the new capability

The key to success is extensive upfront analysis to determine desired capabilities and to plan for staged release of those capabilities based on future upgrades. The process incorporates the relevant changes to the major system acquisition process described previously, but tailored to the unique attributes of information technology and the level of science and engineering technology development (generally very little) required for such systems. Full funding through all phases of deployment is also an essential ingredient for success, so that preplanned

**VULNERABILITY
OF INFORMATION
TECHNOLOGY TO
ENEMY ATTACK
IS THE ACHILLES
HEEL OF U.S.
CONVENTIONAL
FORCES—THERE IS
NO “TECHNOLOGY
SILVER BULLET”
ON THE HORIZON.
THUS, WE
MUST ACQUIRE
INFORMATION
TECHNOLOGY
IN A WAY THAT
CONFOUNDS
THE ENEMY AND
ALLOWS THEM LESS
TIME TO PREPARE.**

program releases can be accomplished. Given the continued need for information technology to improve our nation’s military capabilities—both by using commercial systems and upgrading embedded systems—widespread use of this new process is likely. It should be used when information technology is the dominate acquisition objective, not in cases where hardware development or advances in science or engineering are anticipated.

Cyber security remains an Achilles heel that is inadequately managed in the acquisition process and actively exploited by our adversaries. Many reports by the Defense Science Board and others have highlighted the increased vulnerability of information technology systems to various forms of attack and recommended steps to improve cyber security. (We focus in this report only on those related to acquisition.) While there is no known way to eliminate all vulnerability, DOD can take steps in the short term to minimize the potential for adversary intrusions.

The Department should adopt an acquisition strategy for information technology that confounds the enemy—using variety, change, and rapid acquisition.

In particular, the acquisition approach should incorporate the following features that will make information technology systems more difficult to penetrate:

- ☒ buy in variety and update often
- ☒ buy only needed functionality
- ☒ combine government and commercial off-the-shelf systems
- ☒ create a national defense cyber test bed

Although these features will add cost, the additional cost is necessary. An acquisition strategy without these features is akin to buying a tank without armor—something that would be foolish to do.

The Under Secretary of Defense for Acquisition, Technology, and Logistics should also charter a new study to examine the possibilities for further minimizing information technology

**THE CHAIRMAN,
JOINT CHIEFS OF
STAFF MUST ENSURE
THAT COMBATANT
COMMANDS ARE
TRAINED TO TEST
INFORMATION
TECHNOLOGY
SYSTEMS FOR
AUTHENTICITY
AND TO OPERATE
WITH THEM IN
DEGRADED MODES.**

vulnerabilities and improving information assurance in a more comprehensive manner.

Finally, treat information technology management as a weapon system. Given that the Department's systems are surely to be attacked and degraded, it is important that field commanders develop concepts of operation and tactics, techniques, and procedures that reflect this fact. These concepts should be practiced using exercises to test systems and data for tampering and to develop the necessary skills to operate with systems in a degraded mode.

The Chairman, Joint Chiefs of Staff must ensure that field commanders are trained to test information technology systems for authenticity and to operate with them in degraded modes.

A standing rapid capability fielding organization within DOD would better enable the Department to meet urgent war fighter needs, especially during times of crisis.

DOD lacks the ability to rapidly field new capability to the war fighter in a systematic and effective way.

Currently there are numerous rapid reaction programs and organizations that respond to urgent needs as defined by combatant commanders. It is estimated that these programs spend nearly \$6 billion annually. They are staffed by several hundred people, mostly located in the Office of the Secretary of the Defense; additional rapid fielding capabilities exist throughout the military services as well.

These activities tend to be ad-hoc in formation and one-of-a-kind—such as creation of the Joint Improvised Explosive Device Defeat Organization (JIJEDDO) to focus on the improvised explosive device threat—with little emphasis on training and sustainment requirements associated with fielding. Since these organizations and programs are designed to be temporary, for the purpose of meeting an urgent need, there is little effort to establish institutional memory and no process for “learning” or process improvement. The profusion of independent

CURRENT BUDGET, REQUIREMENTS, AND ACQUISITION PROCESSES, ALONG WITH LONGSTANDING CULTURAL INFLUENCES, MAKE IT DIFFICULT TO QUICKLY RESPOND TO URGENT OPERATIONAL NEEDS ... A STANDING ACQUISITION CAPABILITY IS NEEDED TO FULFILL THESE REQUIREMENTS IN A TIMELY WAY ...

approaches by these organizations can be confusing to contractors and most are supported by funding drawn from the wartime supplements to the DOD budget.

Within OSD, the money and people are dominated by JIEDDO, a classic example of creating a bureaucracy to avoid a bureaucracy. Initially, JIEDDO took a significant amount of time (an average of 9 to 18 months) to sort through ideas, provide development funds, and field initial concepts—with the shorter times requiring workarounds within their own system. Only recently has the output of the organization improved as they have spent significant effort on refining their internal “JCAMP” acquisition process. A more mature acquisition system managed by the Special Forces Command has operated well for several years.

With the exception of the Special Forces Command, these rapid-acquisition organizations have had problems associated with their temporary, ad-hoc nature, but the motivation for their formation has been real. Current budget requirements, longstanding cultural influences, and the overly cumbersome Joint Capabilities Integration Development System (JCIDS) acquisition requirements processes, make it difficult to quickly respond to new urgent operational needs that arise without forming yet another special office or agency. A single, standing acquisition capability, employing the best practices of a consolidation of many of the current rapid organizations, is needed to fulfill these requirements in a timely way, as there is little doubt the need will continue and likely increase.

The Secretary of Defense should create a rapid capability fielding organization to report to the Under Secretary of Defense for Acquisition, Technology, and Logistics. This activity would field capabilities in response to urgent war fighter needs, use an organizational model like the Defense Advanced Research Projects Agency (DARPA), and establish streamlined execution processes.

The principles of operation for such an organization should be as follows:

- ④ It should operate with “colorless” money—allowing resources to be diverted to programs with the most urgent need as they arise.
- ④ The organization should draw on successful attributes, including the somewhat unique culture of DARPA and the acquisition process in the Special Forces Command as organizational models, as well as build on lessons drawn from experiences in other rapid fielding efforts, such as the Mine Resistant Ambush Protected (MRAP) vehicles program.
- ④ The focus of the organization should be on rapid fielding, not acquisition, of time-urgent capabilities. The nature of the needed capability may indeed require acquisition of new capability, but solutions that adapt existing capabilities or tactics, techniques, and procedures should also be part of the scope.
- ④ The staff should comprise a small group of exceptional people who would provide a core capability associated with start-up and support of new initiatives, have the ability to recruit expert project teams tailored to a given initiative, and ensure the dismantlement of those teams once their job is properly completed or transitioned to a Service or other pre-designated owner.
- ④ Consolidated into this activity would be most of the existing OSD rapid fielding initiatives whose mission is still valid, except for JIEDDO.

Expanding on the above points, each project would be approved by the Secretary of Defense. A dedicated, expert project team would then be formed to carry out the project, with a predefined sunset. Once the team completed its mission, it would then execute a transition, negotiated at the project’s inception, to a lead military service who would take on long-term sustainment responsibilities. Each team would implement a single,

time-critical, priority fielding project and have goals focused on solving a specific challenge, without a predetermined solution. The teams would be staffed with a small number of exceptional, can-do people who would call on the expertise of mainstream service organizations—acquisition, logistics, operations and maintenance, training, and others—to execute projects.

While a “DARPA” type model is preferred, we assert that DARPA is not the correct organization to do this. This concept requires a different type of staff with emphasis on fielding, training, program planning, and management rather than the very different activities required for a focus on technology development.

In addition to a very small core staff of typically 20 to 25 individuals, the permanent activity would provide a core of enabling services including recruiting and staffing assistance, office space, contract management, budgeting, accounting, and routine administrative support. Institutional memory would reside with the permanent staff, along with the responsibility of disseminating lessons learned and best practices gained through each project.

4 Improve acquisition execution

COMMERCIAL
ENTERPRISE
CONTINUALLY
DEMONSTRATES
THAT WELL-
RUN PRODUCT
DEVELOPMENT
ACTIVITIES CREATE
NEW PRODUCTS
BETTER, QUICKER,
AND CHEAPER.

Acquisition improvements are not enabled by policy and process reforms alone. Those changes lay the framework for success, but must be coupled with efficient, effective execution led by experienced leaders.

The key improvements in management and execution lie in five areas:

- product development
- contract award and management
- acquisition workforce
- acquisition integrity
- process metrics

Product development is an essential element of acquisition.

Most major acquisition offices have significant difficulty managing the development of new technical capabilities desired in a new platform or system—a challenge that arises for most commercial businesses as well. Commercial entities that are successful link their portfolios of technology development objectives with demonstrations of new capabilities on operational prototypes before a technology is selected for program insertion. In addition, contingency plans are developed for preplanned “workarounds” in case the chosen technology development falls short. Often, with proper planning, the desired technology will be mature enough for insertion in a later block upgrade. This concept, often referred to as “spiral development” in DOD, ensures mature technology for each block, which will ultimately shorten time-to-field, lower risk, and lower cost. These management principles must be used by DOD.

Commercial enterprise continually demonstrates that well-run product development activities create new products better, quicker, and cheaper. DOD needs to change a number of key practices to improve product development.

The Under Secretary of Defense for Acquisition, Technology, and Logistics needs to implement the following practices:

- ❏ change the concept of “requirements” to “capabilities”
- ❏ manage technology development portfolios and create contingency plans for technology insertion
- ❏ maintain persistent technology development prototypes to use as technology demonstrators for sustained systems
- ❏ ensure technology readiness before planned insertion
- ❏ use competitive prototypes when possible
- ❏ use spiral development and block upgrades with stable capabilities for each block
- ❏ give program managers capabilities and performance trade-off authority

Ultimately, the value of the delivered acquisition depends on the capability and performance of the selected contractor and effective contract management.

Although cost and the proposed work plan are clearly critical elements of contractor selection, past performance and relevant experience of the personnel dedicated to the contract are also critical factors in predicting contractor performance. These latter two factors are often found to be missing in troubled programs.

The contract award process sometimes places insufficient weight on past performance and capabilities in contractor evaluation and offers inadequate incentives to encourage contractors to meet program performance, cost, and schedule goals. In fact, often program structures and management actions such as requirement change orders have the unintended effect of rewarding cost growth and schedule delays. The change order process is so common that it encourages and essentially ensures that contractors bid low and plan to “make money on the inevitable change orders.” Contract structures and the tendency for inadequate upfront systems engineering analysis generate opportunities for “requirements” growth and place program managers in

**CONTRACTORS
NEED TO BE
SELECTED BASED
ON THEIR TRACK
RECORD AND THE
EXPERIENCE OF THE
PERSONNEL ON
CONTRACT.**

the vulnerable position of having to negotiate contract changes that generate both cost growth and delays.

The Secretary of Defense should task the Under Secretary of Defense for Acquisition, Technology, and Logistics to issue guidance on contractor selection and management. The contractor selection process should place heavy weight on the management and technical capability of the team dedicated to the project and past performance, as well as the proposed program bid. Competitive prototypes should be used, when feasible, as part of the selection process. Substantial incentives should be established for meeting performance, cost, and schedule goals.

Experienced leadership needs the support of a well-trained and experienced workforce. But, the acquisition workforce in general—both civilian and military—lacks needed experience.

The Office of the Secretary of Defense has lost much of the technical talent needed to oversee the acquisition process. Some talent has been lost due to the large decline in numbers of major programs, some due to ethics and conflict of interest practices that deny access to industry experience, and some due to an aging workforce. The military services face similar challenges. This state of affairs places demands on the acquisition training and education establishment that are well beyond current capabilities, and on the Department's ability to recruit top talent. Strengthening the acquisition workforce is an important priority.

Yet, often the notion of strengthening the workforce is confused with increasing its size. Size is not the important element. In fact, in many cases the actual head count within the acquisition organizations throughout DOD is too high—resulting in too much bureaucracy, overlap and diffusion of responsibilities, lack of accountability, and a requirement for excessive coordination. When an organization is over staffed, the effectiveness and productivity of the workforce tends to decline and managers think they need more people, when in fact they need much fewer. An oversized, inexperienced staff

**OFTEN THE NOTION
OF STRENGTHENING
THE WORKFORCE
IS CONFUSED WITH
INCREASING ITS
SIZE. BUT WHEN
THERE ARE TOO
MANY PEOPLE
“IN THE LOOP”
BUREAUCRACY
MASQUERADES AS
MANAGEMENT.**

requires an enormous amount of coordination among people who do not know what to do or how to do it—and it can take them a long time to decide even the wrong answer. Alternatively, “a few good people” can quickly make the right decision based on experience, and move on.

Previous studies suggest that overstaffing may be several times the number needed in the acquisition workforce. They also show a significant growth in administrative functions relative to war fighting functions. The current acquisition workforce numbers more than 125,000 personnel (25,000 in the Air Force; 45,000 in the Army; 40,000 in the Navy; with the remainder in the Office of the Secretary of Defense and the agencies).² A recent Defense Science Board study showed that the percent of DOD personnel in administrative functions increased from 15 to 23 percent between 1996 and 2005, while the percent of combat soldiers remained nearly constant during the same period. This problem is exacerbated by the rotation policies of the military that tend to move officers through assignments every couple years where nearly half of the time is spent “getting up to speed.”

There is seldom a mature organization in either business or industry that would not be well advised to periodically cut its staff in order to clean out jobs that have outlived their usefulness. In general, we believe the acquisition workforce should be cut by as much as one half—understanding that this is a difficult concept to grasp. Senior executives in both government and industry are accustomed to adding resources to get the job done. But in DOD the issue is the need for more experience rather than higher numbers of people. Experienced professionals are desperately needed to manage acquisition with a broad scope of responsibility and accountability. Such a group of highly capable people, working together as a unit, can learn from each other and form a critical mass that will attract other quality people. The Department has wide flexibility and authority to hire specialists with critical skills (using the Intergovernmental Personnel Act

² Defense Acquisition Workforce Improvement Act (DAWIA) Count Methodology/AT&L Workforce Data Mart (FY 2008) and *Defense Acquisition Structures and Capabilities Review Report*, June 2007.

and other special hiring authorities to draw personnel from industry, other government organizations, and academia), but that authorization is underutilized.

The Under Secretary of Defense for Acquisition, Technology, and Logistics needs to ensure staffing of more experienced civil service and military program managers and program executive officers. This should be achieved by improved training and by hiring individuals with critical needed skills. Managers need to gain experience by managing programs of increasing complexity and scope, and rotating through a variety of program management experiences. At the same time, the overall acquisition workforce needs to be cut in size while giving more accountability and scope of work to the remaining more skilled and experienced staff. With this “right-sized and experienced” workforce and fewer competing organizations, the Department will be creating a coherent, competent, high-quality acquisition staff—one that will attract other like individuals to government service.

Implementing this recommendation is a win-win proposition. The Department could eliminate two to five inexperienced people for each experienced one, saving money on personnel and significantly improving acquisition. Such a program requires experienced leadership to succeed.

As sources for critical military components and designs have become more dependent on global commercial products, the matter of acquisition integrity must gain in prominence.

Commercial design and production trends have increasingly led to sources outside the United States. In response, the DOD acquisition system must incorporate a heightened awareness of the potential harm that can result from a failure to understand the integrity of designs and supply sources.

Many future systems or their components will be of international origin. While international sources of supply may increase vulnerabilities to tampering,

**THE DEPARTMENT
CAN INSTITUTE
PRACTICES FOR
ACQUISITION OF
BOTH HARDWARE
AND SOFTWARE
THAT MITIGATE
VULNERABILITIES.**

domestic supply sources are not immune from insider tampering either. The degree to which defense-unique and commercial material in critical systems are vulnerable should be a major concern. Potential areas where systems may be compromised include: improper design elements and faulty components in integrated circuits and software used in military applications; commercial communications equipment of uncertain origin; and replacement parts for critical aircraft applications lacking the materials properties needed for stressful military use—examples which are by no means exhaustive. In the case of information technology systems, especially software and hardware/software interfaces, there is no way to ensure that the products acquired are in fact only what was desired.

However, the Department can institute practices for acquisition of both hardware and software that mitigate vulnerabilities. In certain cases a controlled DOD source may be preferable provided it can maintain a strong tie to the competitive commercial marketplace.

There is no silver bullet to ensure trusted systems. Hence, a key principle for operators in the combatant commands is awareness. In addition, operators need to test for and monitor system integrity and authenticity; and to plan, train, and exercise for operation in degraded modes.

The Under Secretary of Defense for Acquisition, Technology, and Logistics should develop acquisition processes to: minimize system vulnerability; understand the origin of hardware and software; be willing to pay for controlled sourcing of key components; bring developmental and operational test considerations into the process early; and improve IT security by creating a system that makes it difficult to achieve sustainable penetration.

The Chairman, Joint Chiefs of Staff should direct all military planners and exercisers to recognize the increasing vulnerability of military systems and develop plans; tactics, techniques, and procedures;

and concepts of operations to mitigate the loss of capabilities. Develop processes to detect when systems are degraded and operate accordingly.

Process metrics are essential for measuring improvement and identifying areas of weakness.

There is a well-understood management principle that you can and will only improve what you measure. Managing the acquisition process can only be effective by developing and monitoring process metrics for the reengineered acquisition processes and for the actual performance of acquisition programs. The Secretary of Defense must personally insist on continuous improvement.

The Secretary of Defense, with the Under Secretary of Defense for Acquisition, Technology, and Logistics at the lead, should develop acquisition performance metrics for monitoring the newly reengineered acquisition processes—monitoring each program against performance metrics for cost, schedule, and quality, with quarterly reporting. The metrics should be visible to all. Ensure accountability by developing management reward incentives for program managers who achieve their goals, and be prepared to discipline those who fail.

Finally, the Secretary of Defense needs to ensure that a comprehensive training program is provided to Department and contractor personnel on the entire new acquisition process and agenda. This will help all understand that he does not expect business as usual.

Urgent action is needed

**CONGRESS AND THE
DEPARTMENT MUST
ACT AS PARTNERS
TO "FIX" DOD
ACQUISITION.**

Fixing acquisition is a matter of national security. It is also a tremendous challenge that has plagued many top managers in DOD for decades. While changes to the process have been made in the past, they have met with limited success. This is in large measure because the problem was addressed only at the process level—how to buy. Equally, if not more important, is the need to address the question of what to buy and how the Department makes those decisions.

Fixing the problem calls for attention from the most senior executive in the Department—the Secretary of Defense. To step back and address the matter of what to buy, before focusing on the process of how to buy, is beyond the scope of the acquisition under secretary's responsibilities and requires the Secretary of Defense to take the lead. It is the Secretary who must create a strategic acquisition management platform to guide the Department. And only the Secretary can ensure that it is staffed by the most experienced leaders the nation has to offer.

Congress can and must be part of the solution

Legislation is largely not the problem, but excessive and convoluted regulation and budget instability in programs create turbulence.

As noted earlier, the Department's acquisition performance has given Congress ample reason to step in and "help." Their help is needed now to implement many of the recommendations of this report. For example, to fix DOD acquisition, program funding must be predictable and Congress has to play a critical role in achieving stable program funding. This report calls for new types of funding for acquisition for information technology and for acquisition of the urgent needs that require a rapid acquisition response.

The Department will need support in approving and implementing personnel programs that will enable the Department to hire the right leaders with proven experience. Furthermore, many government requirements (such as the Berry Amendment, Naval Vessel Rules, International Traffic in Arms Regulations, and others)

directly contradict today's commercial design and manufacturing trends. The current rules significantly harm national security options by limiting DOD access to commercial and global technologies and allies' markets. Thus, Congress and the Department must act as partners to "fix" DOD acquisition.

In summary, the key elements of a strategic acquisition platform are as follows:

1. Buy the right things, guided by national security objectives.
2. Select an effective leadership team—in the Office of the Secretary of Defense, the military departments, and defense agencies—with proven, relevant experience. Ensure alignment among senior leadership to DOD goals and timely support of major acquisition decisions.
3. Reform acquisition with efficient processes for major systems, information technology systems, and to rapidly field critical war fighting needs, especially in times of crisis.
4. Improve acquisition execution—management of product development, contract award and management with credible contractor teams and contracts, right sizing and training the acquisition workforce, acquisition integrity, and acquisition performance metrics.
5. Enlist Congress as part of the solution to provide the legislative support needed to succeed.

Even if all the recommendations put forth in this report are implemented, it is recognized that unanticipated problems may arise during the course of any acquisition or product development managed by experienced and well-intentioned people. The only way to minimize the unintended and potentially disastrous consequences of such problems is to quickly recognize and deal with them. If the culture is to use problems as a stick to punish people, then issues will not likely be brought to the forefront in a timely manner and the problems that follow will escalate. DOD acquisition programs are executed on an open stage—creating a difficult job for the best leaders. It is critical that all stakeholders align to deliver our best national security potential.

As threats will surely persist and budgets decline, it will be increasingly important for the Department to streamline its acquisition processes in order to sustain the superior war fighting capability on which the nation depends.

References

Defense Science Board Studies

2008 Summer Study on Capability Surprise (forthcoming).

DOD Policies and Procedures for the Acquisition of Information Technology, March 2009.

Time-Critical Conventional Strike from Strategic Standoff, February 2009.

Integrating Commercial Systems into the DOD, Effectively and Efficiently, February 2009.

Creating an Effective National Security Industrial Base for the 21st Century: An Action Plan to Address the Coming Crisis (DSB Task Force on Defense Industrial Structure for Transformation), July 2008.

Mission Impact of Foreign Influence on DoD Software, September 2007.

2006 Summer Study on Information Management for Net-Centric Operations, April 2007.

2006 Summer Study on 21st Century Strategic Technology Vectors, Volume I, February 2007.

2005 Summer Study on Transformation: A Progress Assessment, Volume I, February 2006.

Management Oversight in Acquisition Organizations, March 2005.

High Performance Microchip Supply, February 2005.

Acquisition of National Security Space Programs (Joint Task Force with the Air Force Scientific Advisory Board), May 2003.

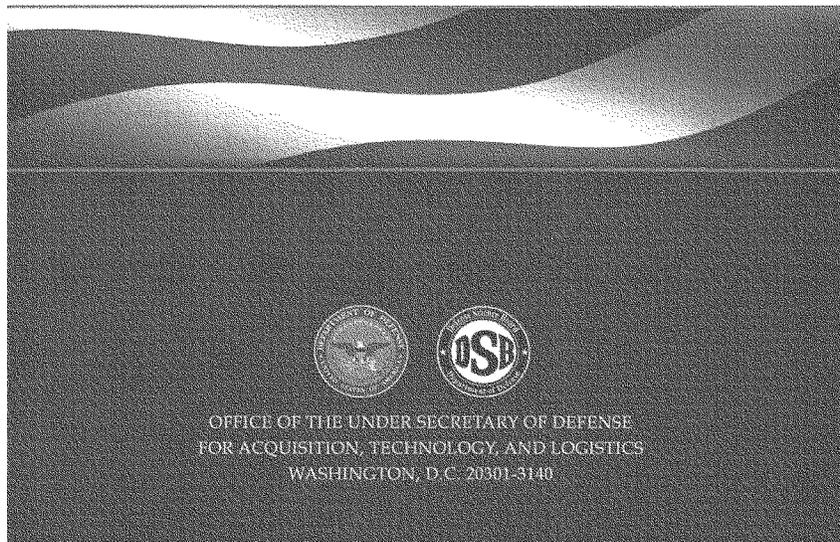
The Impact of e-Business on DOD Acquisition Processes, July 2002.

Other Reports and Articles

A Quest for Excellence (Packard Commission Report), June 1986.

Defense Acquisition University, *Defense Acquisition Structures and Capabilities Review Report*, June 2007.

Fowler, C. A. "The defense acquisition system too late for the scalpel; bring out the meat axe!" *Aerospace and Electronic Systems Magazine*, IEEE, Vol. 9(8), August 1994.





Report of the
Defense Science Board
Task Force on

Department of Defense
Policies and Procedures for the
Acquisition of Information
Technology

March 2009

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a federal advisory committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

The DSB Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology completed its information gathering in December 2008.

This report is unclassified and cleared for public release.

DEFENSE SCIENCE
BOARDOFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

MEMORANDUM FOR: Under Secretary of Defense for Acquisition, Technology
and Logistics

SUBJECT: Final Report of the Defense Science Board Task Force on Department
of Defense Policies and Procedures for the Acquisition of Information
Technology

I am pleased to forward the final report of the Defense Science Board Task Force on Department of Defense (DoD) Policies and Procedures for the Acquisition of Information Technology (IT). This report examines the challenges facing the Department of Defense in acquiring information technology and offers recommendations to improve current circumstances.

The fundamental problem DoD faces is that the deliberate process through which weapon systems and information technology are acquired does not match the speed at which new IT capabilities are being introduced in today's information age. Consequently, the principal recommendation of the study is that the Department needs a new acquisition system for information technology. Roles and responsibilities for those involved in the acquisition process must be clarified and strengthened and the IT system acquisition skills required in the workforce must also be strengthened.

I endorse all of the study's recommendations and encourage you to forward the report to the Secretary of Defense.

William Schneider, Jr.
DSB Chairman



DEFENSE SCIENCE
BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

MEMORANDUM FOR: Chairman, Defense Science Board

SUBJECT: Final Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology

The importance of information technology (IT) to U.S. military capability is widespread. It enables nearly all of the nation's military combat capability and has become a necessary element of our most critical warfare systems. Yet, there is growing concern within Congress and among Department of Defense leadership that the nation's military advantage may be eroding.

At the request of Congress, this task force undertook a review of Department of Defense policies and procedures for the acquisition of information technology. The broad scope of the study touched on acquisition and oversight policies and procedures, roles and responsibilities for acquisition officials department-wide, and reporting requirements and testing as they relate to IT acquisition.

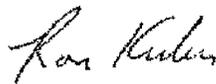
The primary conclusion of the task force is that the conventional DOD acquisition process is too long and too cumbersome to fit the needs of the many IT systems that require continuous changes and upgrades. Thus the task force believes that there is a need for a unique acquisition system for information technology. The task force offers the following recommendations to change the Department's approach to information technology acquisition.

- **Acquisition policies.** A new acquisition process for information technology should be developed—modeled on successful commercial practices, for the rapid acquisition and continuous upgrade and improvement of IT capabilities. The process should be agile and geared to delivering meaningful increments of capability in approximately 18 months or less—increments that are prioritized based on need and technical readiness.
- **Roles and responsibilities of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD (NI)/DOD CIO).** The ASD (NI)/DOD CIO should have strong authorities and responsibilities for enterprise-wide information policy vision, architecture, infrastructure, metadata

and other standards, spectrum, interoperability, information assurance, and system engineering. Some capabilities must be strengthened in order to effectively execute these responsibilities--in particular, system engineering, information assurance, and network integration.

- **Acquisition authorities and organization.** Acquisition authority and expertise in OSD is currently spread across several organizations, resulting in a lack of enterprise-wide architecture and coordination. Consolidate all acquisition oversight of information technology under the USD (AT&L) by moving into that organization, those elements of the ASD (NIH)/DOD CIO and Business Transformation Agency organizations responsible for IT acquisition oversight. (We note that there was not a consensus within the task force concerning this recommendation; a dissenting view is included in appendix A.)
- **Acquisition expertise.** Today, the subject matter competencies required for successful enterprise IT system acquisition are too often missing in government managers responsible for program execution. Acquisition leaders need proven and relevant business experience in the appropriate areas of acquisition, product development, and management. Similarly, program managers and program executive officers need track records of proven success.

The inability to effectively acquire information technology systems is critical to national security. Thus, the many challenges surrounding information technology must be addressed if DOD is to remain a military leader in the future. The development of a new acquisition process, coupled with clear roles and responsibilities of key decision makers, and an experienced leadership and workforce, are important elements of the solution.



Dr. Ronald Kerber
Co-Chair



Mr. Vincent Vitto
Co-Chair

Table of Contents

Executive Summary.....	vii
Chapter 1. Introduction.....	1
Chapter 2. The Information Technology Environment	6
Chapter 3. A Framework for Information Technology Acquisition	25
Chapter 4. Existing Defense Acquisition Process.....	29
Chapter 5. IT Acquisition Challenges and Issues.....	35
Chapter 6. A New Acquisition Process for Information Technology	47
Chapter 7. Summary and Recommendations.....	60
Appendix A. Dissent to Report.....	69
Terms of Reference and Legislative Directive.....	71
Task Force Membership.....	79
Presentations to the Task Force.....	81
Glossary.....	85

Executive Summary

Information technology (IT) offers immense capability in terms of agility, flexibility, responsiveness, and effectiveness. It enables nearly all of our military combat capability and has become a necessary element of our most critical warfare systems. However, there is growing concern within Congress and among Department of Defense (DOD) leadership that the nation's military advantage may be eroding. The deliberate process through which weapon systems and information technology are acquired by DOD cannot keep pace with the speed at which new capabilities are being introduced in today's information age—and the speed with which potential adversaries can procure, adapt, and employ those same capabilities against the United States.

Certainly, barriers that preclude transformation of the U.S. national security apparatus to meet the challenges of a new strategic era are of particular concern. Nearly a decade ago the Department established a vision for the architecture and structure for information system management—a vision that is still evolving. However, it is well known that acquisition has not been well managed for these systems within this “enterprise level” construct, and the result has not served today's leaders and soldiers well. In fact it hinders the war fighters' ability to use information technology to its fullest potential for situation awareness, collaboration, and rapid decision-making. The resulting operational impact is profound.

Yet despite the current situation, successful programs exist that comprise largely or exclusively of information technologies or are deeply dependent on information technology in execution. The question then arises as to whether there are elements common to the acquisition of these successful programs that would improve DOD's ability to field advantageous information technology in a timely and cost-effective manner.

Since the original Goldwater-Nichols legislation, DOD has made several attempts to revise acquisition policy with the hope that such changes would shorten acquisition cycle time. Recently, acquisition policy was again modified in part to add more rigor and discipline in the early part of the acquisition process. Likewise, the Joint Capabilities Integration and Development System (JCIDS) Instruction and Manual are being updated with changes to the Joint Staff's oversight and governance of IT programs. These policies derive from a single

acquisition model that applies to both major automated information systems and major defense weapon systems acquisition programs.

Information technology is pervasive in weapon systems as well as defense business systems. In its contributions to both functionality and cost, IT now represents a considerable proportion of all acquisition programs underway today—a proportion that is likely to increase in the future. Thus, whether existing DOD acquisition policies and processes provide the foundation for an effective information technology acquisition model is a critical question for the Department—one that deserves special attention from the Secretary of Defense.

At the request of Congress, the Defense Science Board (DSB) undertook a review of Department of Defense policies and procedures for the acquisition of information technology. The findings and recommendations presented in this report are the result of a study that was broad in scope, as established in legislative guidance—covering acquisition and oversight policies and procedures, roles and responsibilities for acquisition officials department-wide, and reporting requirements and testing as they relate to IT acquisition.

More specifically, the terms of reference directed that the matters addressed by the task force include the following: 1) DOD policies and procedures for acquiring information technology, 2) roles and responsibilities in implementing policies and procedures, 3) application of acquisition policies and procedures to IT that is integral to critical weapons or weapon system, 4) legal requirements (U.S. Code) as they relate to the acquisition of IT, 5) DOD policies and procedures to facilitate the use of commercial information technology, 6) suitability of DOD acquisition regulations, 7) adequacy and transparency of metrics, 8) effectiveness of existing statutory and regulatory reporting requirements, 9) adequacy of operational and development test resources, and 10) appropriate policies and procedures for technology assessment, development, and operational testing.

Based on the expertise of the task force members and information briefings received during the course of its deliberations, **the task force believes that there is a need for a unique acquisition process for information technology.** Such a process must be designed to accommodate the rapid evolution of information technologies; their increasingly critical position in DOD warfare systems, warfare support systems, and business systems; and the ever evolving and often urgent IT needs of our war fighters. The conventional process, with its recent improvements, would be used when a system requires

significant scientific or engineering technology development, particularly hardware development or the integration of many complex systems requiring design and functionality partitioning and trade-offs.

Problems that plague IT acquisition are similar to those that plague the acquisition of major systems, most of which have a high content of embedded IT. **The conventional DOD acquisition process is too long and too cumbersome to fit the needs of the many systems that require continuous changes and upgrades**—a reality driven by the short half-life of commercial IT, supportability of hardware (which is often a commodity), software applications, and operational requirements. Thus, the Department's leaders must take action to address this problem. Toward that end, the task force offers the following recommendations to change the Department's approach to information technology acquisition.

Statutory Restrictions

The task force believes that the statutory framework is workable and is not a major impediment to improving IT acquisition within DOD. Therefore, no recommendations are offered in this area. The main issue with regard to statutory influence is that Congress has lost confidence in DOD's execution of IT programs, which has resulted in increasing program scrutiny and budget actions (generally funding cuts) for programs that are faltering. Since DOD implementation of IT acquisition has fallen short, Congress has added additional constraints on reporting and management; these could become problematic when and if DOD begins executing programs well.

Acquisition Policies

Acquisition policies (DOD Directive 5000.1 and Instruction 5000.2) are principally designed for programs where technology development for hardware and software is a critical component. The recent revisions to DOD Instruction 5000.02, implemented December 2008, offer improvements to the process but do not address the fundamental challenges of acquiring information technology for its range of uses in DOD. Instead, a new acquisition approach is needed that is consistent with rapid IT development cycles and software-dominated acquisitions.

RECOMMENDATION 1. NEW ACQUISITION PROCESS FOR INFORMATION TECHNOLOGY

The Secretary of Defense should:

- Recognize that the current acquisition process for information technology is ineffective. Delays and cost growth for acquisition of both major weapons systems and information management systems create an unacceptable risk to national security.
- Direct the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)) and the Vice Chairman, Joint Chiefs of Staff, to develop new acquisition and requirements (capabilities) development processes for information technology systems. These processes should be applicable to business systems, information infrastructure, command and control, ISR (intelligence, surveillance, and reconnaissance) systems, embedded IT in weapon systems, and IT upgrades to fielded systems.
- Direct that all personnel within the Office of the Secretary of Defense (OSD), the Joint Staff, and the Services and agencies involved with acquisition be accountable to ensure that their efforts are focused on the improvement, streamlining, and success of the new process.

The USD (AT&L) should lead an effort, in conjunction with the Vice Chairman, Joint Chiefs of Staff, to develop new, streamlined, and agile capabilities (requirements) development and acquisition processes and associated policies for information technology programs.

The task force proposes a new process, modeled on successful commercial practices, for the rapid acquisition and continuous upgrade and improvement of IT capabilities (Figure FX-1). The process is agile, geared to delivering meaningful increments of capability in approximately 18 months or less, and leverages the advantages of modern IT practices. Multiple, rapidly executed releases of capability allow requirements to be prioritized based on need and technical readiness, allow early operational release of capability, and offer the ability to adapt and accommodate changes driven by field experience.

The process requires active engagement of the users (requirements) community throughout the acquisition process, with requirements constructed in an enterprise-wide context. It is envisioned that requirements will evolve so “desired capabilities” can be traded-off against cost and initial operational capability to deliver the best capability to the field in a timely manner. A modular, open-systems methodology is required, with heavy emphasis on “design for change,” in order to rapidly adapt to changing circumstances. Importantly, the process needs to be supported by highly capable, standing infrastructure comprising robust systems engineering, model-driven capability definition, and implementation assessments—to reduce risk, speed progress, and increase the overall likelihood of repeated successes. Early, successive prototyping is needed to support the evolutionary approach. In addition, key stakeholders—the Chief Information Officer (CIO), Program Analysis and Evaluation (PA&E), Director of Defense Research and Engineering (DDR&E), Operational Test and Evaluation (OT&E), the Comptroller, operational users, and others—need to be involved early in the process, prior to the milestone build decision.

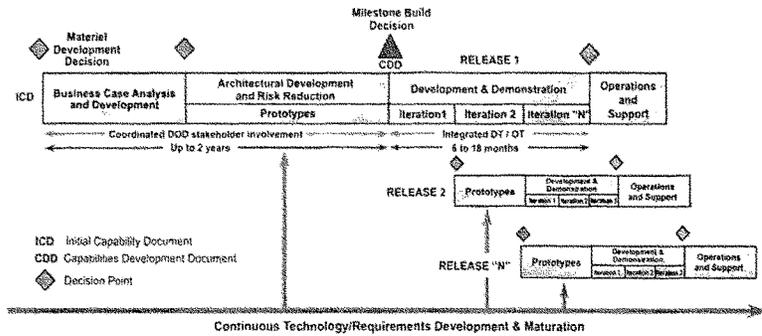


Figure EX-1. A New Acquisition Process for Information Technology

Testing methodologies and procedures need to be engaged early and often in the acquisition process, with integrated and continuous development and operational testing practiced during the development and demonstration phase for each capability release. Contracting vehicles need to be devised that are flexible enough to support this agile process. These vehicles must allow for changes in delivered capability within a particular increment, as well as allow

capability to be deferred to subsequent increments if needed. Crucial to the success of a new process is continuity of funding, to maintain a solid funding stream for following, sometimes overlapping, capability releases. Along with the flexibility built into the process, relevant metrics, similar to those used in commercial practice, are needed to continuously track IT acquisitions to ensure that the expected capability is being provided, costs are being managed, and the schedule to initial capability is on track. Finally, just as there is no substitute for acquisition leadership experience in DOD, the same is true for the contractor community. For contact award, program managers need to strongly consider relevant contractor experience and past performance, especially in large acquisitions, and ensure that key personnel are committed for the duration of the project.

The task force believes that this new process will have applicability over a broad range of new DOD IT acquisitions and upgrades to existing national security systems (including command and control systems), IT infrastructure, and other information systems (Figure EX-2). IT is not simply a niche consideration—it touches a wide range of systems and, in turn, enables a wide range of capabilities.

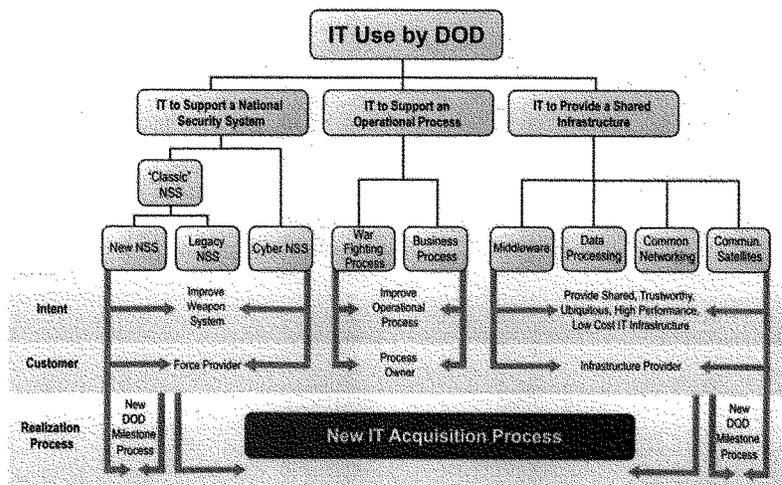


Figure EX-2. An Information Technology Acquisition Framework

Deciding When to Use the New IT Acquisition Process

It is important to clarify when to use the new IT acquisition process versus the improved DOD 5000.02 process for major weapon systems and communication satellites. In addition, it is also necessary to reduce potential confusion about technology development.

The use of the improved DOD 5000.02 process for major weapon systems is required when there are many design trade-offs for hardware and IT systems and for partitioning the functions and interoperability of embedded IT systems and subsystems in a new system, while assuring interoperability and network compatibility with the larger enterprise. At the same time there are likely to be areas of needed technology development that require advances in science and engineering that have little or nothing to do with IT—such as new material properties, increased speed, or stealth. This later scientific and engineering technology development should not be confused with the traditional jargon of the IT community that defines technology development nearly interchangeably with software development and hardware integration.

The use of the new IT acquisition process is for new or replacement stand alone IT systems and subsystems or for replacement IT systems embedded in existing weapon systems that are to be upgraded when there is little or no change in the hardware not associated with IT. It may also be appropriate to use the IT acquisition system process concept within the 5000.02 process for new embedded IT systems in a major weapon system acquisition as the IT technology could otherwise be a few generations old when the system is fielded.

While one could argue that this required new decision could add confusion to the process, one could also argue that if the leadership and program managers cannot sort out this high-level decision they have no chance of effectively managing or overseeing the program.

Roles and Responsibilities of the ASD (NII)/DOD CIO

Developing and implementing an acquisition process for information technology is an important step toward reducing delays and cost growth in information technology programs, as well as providing capability more rapidly to the war fighter. Perhaps equally important, however, is clarifying roles and responsibilities of the key players in the process—chief information officers and

those individuals who hold milestone decision authority (discussed in the next section).

The DOD CIO function is currently housed in the Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (OASD (NII)/DOD CIO). DOD CIO responsibilities are delineated within titles 10, 40, and 44 of the U.S. Code. As designated in legislation, the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD (NII)/DOD CIO) reports directly to the Secretary of Defense—a reporting chain that the task force believes is critical and must continue in order for the ASD (NII)/DOD CIO to have the necessary authority to carry out important Department-wide functions.

The ASD (NII)/DOD CIO should have strong authority and responsibility for information policy vision, architecture, infrastructure, standards, spectrum, information assurance, interoperability, and enterprise-wide systems engineering. The ASD (NII)/DOD CIO should be the Department's single authority for certifying that IT acquisitions comply with an enterprise-wide architecture and should continually review ongoing programs for architectural compliance. He or she should also be a ruthless designer of "the enterprise" infrastructure and should approve IT program manager training and certification.

These functions are also applicable to CIOs at the Service and agency level. To execute the above responsibilities, Service and agency CIOs should also directly report to the head of the Service or agency, as required by legislation.

However, the task force believes that some of the functions delineated above need to be strengthened in order to ensure that the full responsibilities of the office can be effectively executed.

RECOMMENDATION 2. ASD (NII)/DOD CIO RESPONSIBILITIES

The ASD (NII)/DOD CIO should actively exercise his or her authority to certify that all IT acquisitions are consistent with the Department's net-centric architecture.

The ASD (NII)/DOD CIO should have strong authority and responsibility for enterprise-wide information policy vision, architecture, infrastructure, metadata and other standards, spectrum, interoperability, information assurance, and system engineering.

Certain capabilities in the OASD (NII)/DOD CIO must be strengthened in order to more effectively execute these responsibilities—in particular, system engineering, information assurance, and network integration.

In the Services and agencies, the CIOs should also have strong authorities and responsibilities for system certification, compliance, applications development, and innovation.

All CIOs should approve IT acquisition program manager training and certification and advise the personnel selection process.

The DOD CIO, supported by CIOs in the Services and agencies, should be responsible for certifying that systems and capabilities added to the enterprise do not introduce avoidable vulnerabilities that can be exploited by adversaries.

Both system vulnerability to sophisticated adversary threats and information and mission assurance should be addressed throughout program development, particularly in the early stages during the business case analysis and development phase. As new capabilities, infrastructure, and applications are added to a system, this same assessment should be continuously monitored with particular emphasis on source code analysis and supply chain risk assessment. A robust testing program must also be established to minimize the introduction of new vulnerabilities. New capabilities need to be tested in realistic test beds under a variety of threat scenarios.

While not the centerpiece of this report, the task force believes that information and mission assurance must be an integral element of the IT acquisition process, not an afterthought. IT is far too important to the Department's war fighting and business endeavors to neglect information and mission assurance, as the consequences of doing so can not only undermine the current system but also other connected capabilities as well. In this context, it is instructive to remember that there is no way to test a large IT system to assure that you "got what you wanted" and only what you wanted. Thus, since it is not possible to assure that an IT system is entirely safe and reliable, operators (combatant commanders) must develop field testing procedures; tactics, techniques, and procedures; and concepts of operations to operate with degraded systems.

Milestone Decision Authority Roles and Responsibility

Clear roles and responsibilities of those with milestone decision authority are essential if a new acquisition process is to be successful and the desired outcomes achieved. The lack of clarity in this regard is one of the most significant impediments to successful implementation of the current process. The task force believes that the preferred approach should be delegation to the lowest level acquisition decision authority, consistent with program risk.

Furthermore, acquisition authority and expertise within OSD is currently spread across several organizations—under the USD (AT&L), in OASD (NII)/DOD CIO, and in the Business Transformation Agency. At the Service level, similar disaggregation of responsibility also exists. This disaggregated approach seems inefficient to the task force, resulting in a lack of enterprise-wide architecture and coordination. Qualified IT acquisition and systems analysis and architecture personnel are scarce and should not be spread among separate OSD organizations. Given the speed with which information technology advances, this disaggregation exacerbates the ability to maintain currency and coordination within the acquisition workforce.

It is important to recognize that IT acquisition requirements are different and, because IT touches nearly everything acquired by the Defense Acquisition Executive (the USD (AT&L)), it is more than a side consideration. Bringing together the expertise from many organizations into a single one will help to ensure that the unique attributes of IT programs are better understood. In addition to milestone decision authority responsibilities and organization, the Defense Acquisition Executive advisory staff (DDR&E, PA&E, OT&F, Comptroller) issue definition and resolution process often contributes to extended IT acquisition times.

RECOMMENDATION 3. ACQUISITION AUTHORITIES AND ORGANIZATION

The USD (AT&L) is responsible for all acquisitions, the acquisition workforce, and is the milestone decision authority for all major defense acquisition programs (MDAP), major automated information systems (MAIS), and special interest programs. The USD (AT&L) should:

- aggressively delegate milestone decision authority commensurate with program risk

- consider a more effective management and oversight mechanism to ensure joint program stability and improved program outcomes

Consolidate all acquisition oversight of information technology under the USD (AT&L) by moving into that organization those elements of the OASD (NII)/DOD CIO and Business Transformation Agency responsible for IT acquisition oversight. The remainder of OASD (NII)/DOD CIO is retained as it exists today, but should be strengthened as indicated in the previous recommendation.

Acquisition Expertise

A high degree of relevant technical and proven management capability is needed for IT system acquisition leadership. In addition, a set of IT domain experts are needed within the acquisition community to support acquisition oversight and decision-making. OSD and the Services need IT acquisition staff with extensive experience in large-scale, embedded, and commercial IT.

Today, the subject matter competencies required for successful enterprise IT system acquisition are too often missing in government managers responsible for program execution. Skills in program administration are confused with skills in operational process design and/or with skills in IT. Contracting, budgetary, and organizational design debates crowd out concepts of operations and system engineering debates. Further, architecture is too often viewed as a paper exercise rather than a model-driven, analytically supported, and rigorous engineering process incorporating enterprise-wide considerations for functionality and interface definition. Within the Department, IT expertise is scarce and the competition for talent is increasing.

There is no substitute for experienced program managers with track records of proven success. In a review of major IT acquisition programs where cost, schedule, or quality and performance were issues, three root causes emerged. First, senior leaders lacked experience and understanding. Second, the program executive officers and program managers had inadequate experience. Third, the acquisition process was bureaucratic and cumbersome, where many who are not accountable must say “yes” before authority to proceed is granted. Among these problems, lack of experience dominated.

The experience and qualifications of OSD and Service leaders, and program executive officers and program managers is critical to making the *right judgments* to begin a program with executable objectives and then manage it to successful completion.

RECOMMENDATION 4. ACQUISITION EXPERTISE

The Secretary of Defense shall require that the Defense Acquisition Executive (USD (AT&L)) and the component acquisition executives have proven and relevant business experience in the appropriate areas of acquisition, product development, and management. Such qualifications apply to the ASD (NII)/DOD CIO and Service and agency CIOs as well.

The USD (AT&L) must work with Service and agency acquisition executives to improve the capabilities and selection process for program executive officers and program managers.

The USD (AT&L) shall direct the Defense Acquisition University, in coordination with the Information Resources Management College, to integrate the new acquisition model into their curriculum.

Conclusion

The bottom line is that the inability to effectively acquire IT systems is critical to national security. Today the United States has the most capable fielded war fighting systems in the world. Information technology is critical to a wide range of capabilities: command and control, decision systems, precision weapons, and situation awareness. The task force found that performance of the Department's current IT acquisition process is not acceptable. Thus, the many challenges surrounding information technology must be addressed if DOD is to remain a military leader in the future.

The task force believes that actions in the four areas discussed above—acquisition policies and process, roles and responsibilities of the CIO, milestone decision authority roles and responsibilities, and acquisition leadership expertise—will improve the acquisition of information technology in DOD. But caution is offered that emphasis and focus only on the acquisition process is not enough. While the task force feels that a new process is needed that better takes

into consideration the unique aspects of information technology, it alone will not yield success. If the matters associated with responsibilities and authorities, organization, and expertise are not also addressed, the new process proposed here is likely to meet with the same outcomes as process improvements recommended by other groups who have studied this issue. This set of recommendations is designed to both streamline the IT acquisition process and address the fundamental problems that exist in the system today.

Chapter 1. Introduction

Information technology (IT) offers immense capability in terms of agility, flexibility, responsiveness, and effectiveness. IT enables nearly all of our military combat capability and has become a necessary element of our most critical warfare systems. However, there is growing concern within Congress and among Department of Defense (DOD) leadership that the nation's military capability may be eroding. The deliberate process through which weapon systems and information technology are acquired by DOD cannot keep pace with the speed at which new capabilities are being introduced in today's information age—and the speed with which potential adversaries can procure, adapt, and employ those same capabilities against the United States. For purposes of clarity, IT, as defined in this report, is any system or subsystem of hardware and/or software whose purpose is acquiring, processing, storing, or communicating information or data. DOD has a very long definition of IT which is too complicated to be useful.

Certainly, barriers that preclude transformation of the U.S. national security apparatus to meet the challenges of a new strategic era are of particular concern. Nearly a decade ago the Department established a vision for the architecture and structure for information system management—a vision that is still evolving. However, acquisition decision-making has not been well managed for these systems within this “enterprise level” construct, and the result has not served today's leaders and soldiers well. It hinders the war fighters' ability to use information technology to its fullest potential for situation awareness, collaboration, and rapid decision-making. The resulting operational impact is profound.

According to the Defense Science Board 2006 Summer Study on Information Management for Net Centric Operations, information management in Iraq and Afghanistan was a principal concern among war fighters. Significant ad hoc activity was taking place, especially at the tactical level, to gain desired capability. To counter the interoperability problem, many approaches were used to move information from one stove-pipe to another. Especially important, according to the 2006 report, was that much of the military capability used to support the conflicts was paid with supplemental funding—programs that were not part of the Department's planned capability. This circumstance reflects the fact that the need for such programs could not be predicted during previous core

program and budget planning, and the system was not sufficiently agile to react once the need was apparent.

Yet, despite these myriad obstacles, successful programs exist that are comprised largely (or exclusively) of information technologies, or are deeply dependent on information technology in execution. The question then arises as to whether there are elements common to the acquisition of these successful programs that would improve the Department's ability to field advantageous information technology in a timely and cost-effective manner.

Since the original Goldwater-Nichols legislation, DOD has made several attempts to revise acquisition policy with the hope that such changes would shorten acquisition cycle time. Recently, acquisition policy was again modified in part to add more rigor and discipline in the early part of the acquisition process. Likewise, the Joint Capabilities Integration and Development System (JCIDS) Instruction and Manual are being updated with changes to the Joint Staff's oversight and governance of IT programs. These policies derive from a single acquisition model that applies to both major automated information systems and major defense acquisition programs.

Information technology is pervasive in weapon systems as well as defense business systems. In its contributions to both functionality and cost, information technology now represents a considerable proportion of all acquisition programs underway today—a proportion that is likely to increase in the future. Thus, whether existing DOD acquisition policies and processes provide the foundation for an effective acquisition model for information technology is a critical question for the Department—one that deserves special attention from the Secretary of Defense.

At the request of Congress, the Defense Science Board (DSB) undertook a review of Department of Defense policies and procedures for the acquisition of information technology. The task force offers recommendations to change the Department's approach to acquiring information technologies. The findings and recommendations are the result of a study that was broad in scope, as established in legislative guidance—covering acquisition and oversight policies and

procedures, roles and responsibilities for acquisition officials department-wide, and reporting requirements and testing as they relate to IT acquisition.¹

More specifically, the terms of reference directed that the matters addressed by the task force include the following:

1. **DOD policies and procedures for acquiring information technology**, to include national security systems, major automated information systems, business information systems, and other information technology.
2. **Roles and responsibilities in implementing policies and procedures of the:**
 - Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L))
 - DOD Chief Information Officer
 - Director of the Business Transformation Agency
 - service acquisition executives
 - Chief Information Officer of the military departments
 - defense agency acquisition officials
 - information officers of the defense agencies
 - Director, Operational Test and Evaluation and heads of the operational test and evaluation organizations of the military departments and the defense agencies
3. **Application of such policies and procedures to information technologies that are an integral part of critical weapons or weapon systems.**
4. **Requirements of subtitle III of title 40, U.S.C. and chapter 35 of title 44, U.S.C.** regarding performance-based and results-based management, capital planning, and investment control in the acquisition of information technology.

1. Acquisition programs under authority of the Under Secretary of Defense for Intelligence are outside the scope of this study.

5. **Department of Defense policies and procedures for maximizing the usage of commercial information technology** while ensuring the security of the microelectronics, software, and networks of the Department.
6. **Suitability of DOD acquisition regulations**, including DODD 5000.1, DODI 5000.2, and accompanying milestones, to the acquisition of IT systems.
7. **Adequacy and transparency of metrics** used by DOD for acquiring IT systems.
8. **Effectiveness of existing statutory and regulatory reporting requirements** for acquisition of IT systems.
9. **Adequacy of operational and development test resources** (including infrastructure and personnel), policies, and procedures to ensure appropriate testing of IT systems both during development and before operational use.
10. **Appropriate policies and procedures for technology assessment, development, and operational testing** for purposes of adopting commercial technologies into IT systems.

Based on the expertise of the task force members and information briefings received during the course of its deliberations, **the task force believes there is a need for a unique acquisition system for information technology.** Such a process must be designed to accommodate the rapid evolution of information technologies; their increasingly critical position in DOD warfare systems, warfare support systems, and business systems; and the ever-evolving and often urgent IT needs of our war fighters.

The issues associated with the acquisition of IT systems are a subset of similar problems the Department faces in acquiring major weapon systems, most of which have a high content of embedded IT. A common theme to all is that continuous changes and upgrades are a reality and must be accommodated—a reality driven by the short half-life of commercial IT technology, supportability of hardware (which is often a commodity), software applications, and operational requirements. **The conventional DOD acquisition process is too long and too cumbersome to fit the needs of the many systems that require continuous changes and upgrades.** Many existing programs are exceeding cost and schedule baselines, which cannot continue unabated. While the task force recognizes that there is no “one-size-fits-all” solution to DOD’s acquisition

problems, it also believes there is merit in minimizing the number of specialized acquisition approaches. That said acquisition of information technology represents a case that must be addressed with a process that focuses on the unique characteristics IT represents.

The bottom line is that the inability to effectively acquire IT systems is critical to national security. Today, the United States has the most capable fielded defense systems in the world, and information technology is critical to these capabilities—to command and control, decision systems, precision weapons, and situation awareness. Spending on IT is rapidly growing in both embedded and stand-alone systems. As well, IT system acquisition and IT upgrades to existing weapon systems represent a significant and growing percentage of current acquisitions. Further, inadequate attention to cyber security in the acquisition process is an Achilles heel that can be actively exploited by our adversaries. While this report does not address cyber security in any detail, it does highlight the need to keep this critical issue in mind both during IT acquisition and through operational procedures in the field. These many challenges surrounding information technology must be addressed if DOD is to maintain our national security objectives as a military leader in the future.

The chapters that follow detail the work of the task force, leading up to a set of actions for DOD. Chapter 2 begins with an overview of the information technology environment, followed in Chapter 3 by a framework for evaluating IT acquisition. Chapters 4 and 5 focus on the existing acquisition system and the problems that arise with the acquisition of IT programs. Chapter 6 proposes a new acquisition process for information technology. The report concludes in the final chapter with key findings and recommendations.

Chapter 2. The Information Technology Environment

Information technology is pervasive throughout DOD systems, from infrastructure to business systems to IT embedded in weapon systems. Whereas in 1970 software accounted for about 20 percent of weapon system functionality, by 2000 it accounted for as much as 80 percent² and today can deliver 90 percent³ or more of a system's functionality. While its importance is growing, the information technology environment is experiencing a disturbing set of trends (Figure 1).

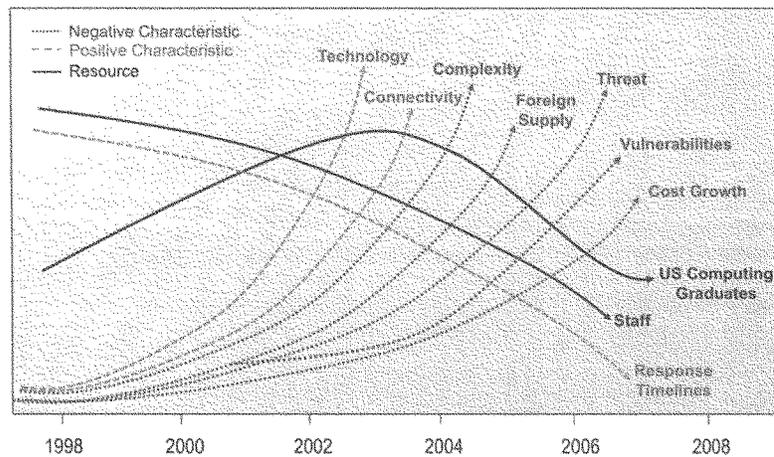


Figure 1. The Perfect IT Storm

2. Defense Science Board Task Force on Defense Software. November 2000.

3. *Program Manager's Guide for Managing Software*, October 10, 2001, Rev 2.0 <https://acc.dau.mil/CommunityBrowser.aspx?id=24374&clang=en-US>

These trends include an increase in IT complexity, foreign supply, vulnerabilities, threats, and cost with a concomitant reduction in the supply of U.S. computing graduates and qualified expert government staff. Simultaneously, the rate of technology change is increasing as is the interconnected nature of systems, while timelines are shrinking—circumstances that pose both a benefit and risk to DOD. Each of these key trends and their implications is detailed in the remainder of this chapter.

Technology Change

Information technology—from hardware to software to complex systems—continues to rapidly advance. Computer hardware rapidly evolved from vacuum tubes to transistors to nanotechnology. In his 1965 paper, Intel co-founder Gordon E. Moore predicted that the number of transistors on an integrated circuit board would increase “at a rate of roughly a factor of two per year.” In 1975, Moore refined his projection to a doubling every two years. Still known as Moore’s Law (Figure 2), this exponential growth has held for processing speed, memory capacity, and even the number and size of pixels in digital cameras.⁴ While Moore’s Law has held for decades, processing speed is no longer increasing at this rate. Instead the industry has moved to a multi-core approach. Unfortunately, parallel processing software has lagged behind. This will be an important trend for DOD to monitor and understand.

In addition to changes in hardware, IT architectures have evolved over the past several decades from isolated computing systems of the 1960s; to networked stovepipes in the 1970s and 1980s; to the use of message passing middleware to glue together mission applications in the 1990s; to the open, service-oriented architectures (SOA) of today (Figure 3). SOA is a method for organizing, exposing, and utilizing distributed capabilities that may be under the control of different ownership domains. This evolution toward the disaggregation of systems into distributed services promises more rapid development, reuse, and survivability, yet at the same time increases interdependencies, vulnerabilities, and complexity (and possibly impacts performance). The impact of this evolution is underestimated. It will allow substantial change in the nature and substance of IT acquisitions by further enabling the rapid development and fielding of small increments of capability.

4. Dale W. Jorgenson and Charles W. Wessner. 2006. (eds). *Measuring and Sustaining the New Economy, Software, Growth, and the Future of the U.S. Economy: Report of a Symposium*. National Research Council. Figure 1, p. 6. www.nap.edu/catalog/11587.html

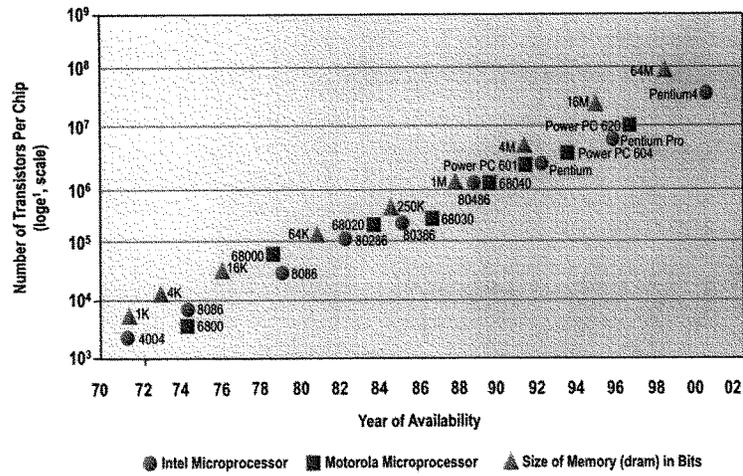


Figure 2. Moore's Law: Transistor Density on Microprocessor and Memory Chips

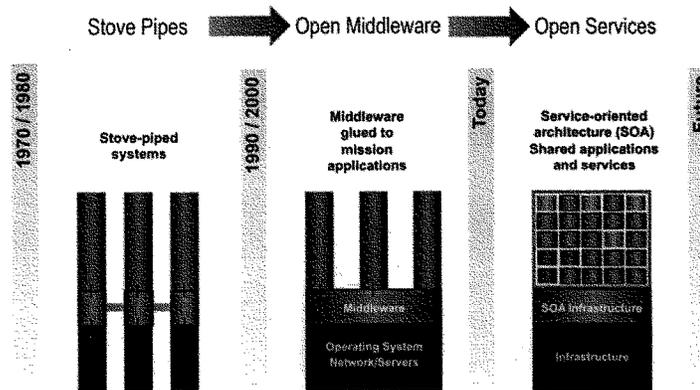


Figure 3. Evolution of Information Technology Architectures

While initial attempts to expose and standardize large amounts of data and metadata about legacy systems have proved highly complex and time intensive, one method that has successfully emerged is known as “loose coupling” in which minimal but critical data interfaces are exposed to support interoperability. For example, Cursor on Target,⁵ a machine-to-machine language designed to communicate battlefield information, enables rapid but minimal integration of a few crucial data elements (e.g., position, time, object, event) across legacy systems. In summary, technology will continue to rapidly evolve, imposing challenges for personnel and programs to remain current.

Disaggregated Architectures

DOD’s II’ vision includes one very special feature—the separation of data from services and applications. This separation provides two high-priority benefits.

- It supports the introduction of new applications and/or services without requiring a lengthy, expensive N-squared, application-to-application integration.
- It enables operators to discover, use, publish, and govern data in ways that were not planned or anticipated on an operational, as-needed basis.

While the introduction of disaggregated architectures and the separation of data from applications and services will provide significant benefits to the Department in both development and operations, the planned outcome is a very different environment. Reaping these benefits will require rethinking and modifying the Department’s processes.

From an architecture perspective, it is likely that the disaggregated model will not directly support all of the Department’s low latency requirements in the near-term. The solution to this appears to be relatively straightforward. Simply allow low latency applications to receive data on a “push” rather than a “pull” basis, while at the same time, require the data sources to post their data in parallel for other uses/users. This approach will require: 1) development of the criteria for deciding which systems have such stringent low latency requirements (e.g., fire control systems) that they will be allowed to obtain data on a “push” basis, and

5. Miller, R. and Winkowski, D. *Loose Couplers as an Information Design Strategy*. www.ffrdc.org/work/tech_papers/tech_papers_07/07_0802/07_0802.pdf

2) sorting out which systems are expected to provide data for use by these same systems.

This solution is not ideal for this set of systems, as it will not provide all of the benefits of a disaggregated environment where data is separated from applications, services, and governance. It is also clear that not all of the information security requirements will be addressed by the IT infrastructure; some of these requirements must be addressed within the mission applications or services. While this should not be a surprise, it is worth noting since the goal is to have as many of the enterprise functions performed by the infrastructure as possible, in order to facilitate the introduction of new applications and services.

There are also some implications from acquisition and implementation perspectives. While there are significant benefits to being able to implement new applications and services quickly, the acquisition process will need to support these quick turn efforts more easily than it does today (which will be discussed in more detail in later chapters of this report). To deliver acceptable quality of service and to support the information and the network security required by DOD in an enterprise-wide SOA, with enterprise-wide access to data by authorized users, a well engineered and governed enterprise IT infrastructure is essential.

However, creating an enterprise infrastructure is not trivial. Transitioning from the existing platform/system and occasionally enclave-based environment, to an enterprise IT infrastructure will put additional stress on the Department, especially on the technical management and acquisition process. For example, the test process will have to change to allow DOD to speed application and service implementations. At the same time there will be differences for the test function, as tests must be performed on both the infrastructure and on the individual applications/services. Both are required to deliver capabilities, but the test timelines should be very different.

There will also be funding challenges. The Department's three core processes—requirements, acquisition, and resourcing—are just starting to move from platforms to capabilities, although the focus on individual capability delivery increments still dominates. Adoption of a service-oriented architecture and institutionalization of an enterprise-wide IT environment will require a significant investment in the infrastructure itself. The good news is that implementation can be segmented over time and purpose. Individual applications

and services that will ultimately rely on the infrastructure must trust that it will be successfully funded and developed.

Two additional matters relate to funding this “common good.” One is the need to expose and maintain data for unanticipated users, which is necessary to avoid an erosion of confidence in the enterprise-wide environment. A second is that building and delivering a reusable service clearly provides a cost benefit if the service is reused, but can require additional funds for the developer that must increase support for unplanned users from other parts of the organization.

Connectivity

Just as we are experiencing rapid technology change, we are also facing rapid global increases in connectivity among computers and, consequently, among people. There are already nearly one and one half billion Internet users. By 2012, one quarter of the world population will have regular access to the Internet.⁶ Brazil, Russia, India, and China are experiencing some of the highest growth rates.

More important than growth in the raw numbers of users is the belief that their collective power increases exponentially with the number of nodes. Robert Metcalf, founder of 3Com Corporation, noted that the value or utility of a network is equal to the square of the number of nodes (e.g., the number of connected individuals)—the so called Metcalf’s Law (Figure 4). Whether the value grows as Metcalf’s law, as $n(\log(n))$ as some researchers now believe, or as Reed’s law, which states that it grows faster due to forming communities of interest as is beginning in DOD, is not as important to understand as the fact that the value is growing in a highly nonlinear way with respect to size.

The Department of Defense has recognized and capitalized on the potential of net centricity. The Global Information Grid (GIG) is a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand for the Department of Defense. As of 2008, the GIG incorporated 21 satellite communications networks; 65 nations; over 3,500 bases/posts; approximately 15,000 networks; thousands of applications; 120,000 commercial telecommunications circuits; and 7 million DOD computers (twice

6. Schgal, V. June 3, 2008. *Concept Report*. Worldwide Online Population Forecast, 2007 to 2012. JupiterResearch.

as many as in 2005). While the size and ubiquity of this ever growing enterprise is a challenge in itself, additional IT functionality and increased cross-organization, coalition, and security boundary connectivity further exacerbates the enterprise challenge.

Most importantly, but easily overlooked, is that achieving “the power of networks” requires the elements of the network to be constructed according to widely accepted and adopted standards, and executed in accordance with an overarching network architecture concept and design. Chaotic creation of “networks” and/or “network nodes” will not yield the benefits promised by Metcalf’s Law. The underlying proposition is that adoption of standards increases the ability to “connect,” which gives encouragement to increase the number of connectors. In turn, this enables an increase in the information exchanged as well as the utility and value of information exchanged within and among the network(s).

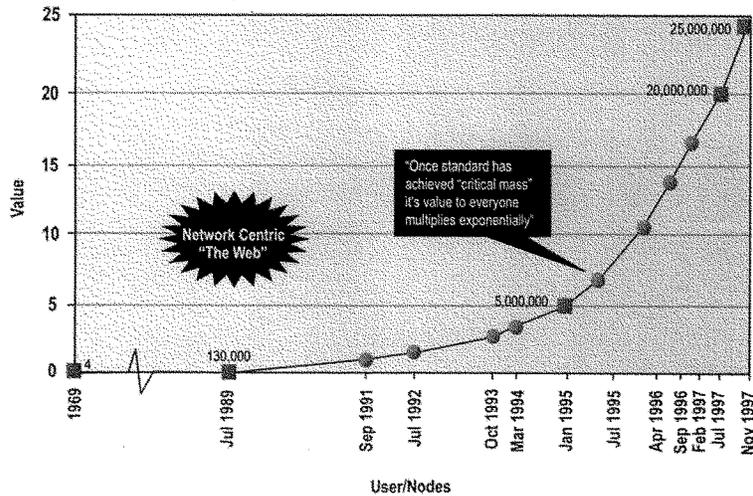


Figure 4. Metcalf's Law: The Power of a Network

Size and Complexity

While the sheer number of nodes (computers, routers, business systems, weapon systems) and connections among nodes in the GIG is increasing dramatically, the underlying software code base is growing, driving complexity of design, operation, protection, and maintenance. This is occurring both in infrastructure software, as well as in weapon systems software. For example, the most ubiquitous commercial operating system (Microsoft Windows) has grown from thousands of lines of code (LOC) to tens of millions (left graphic below)⁷ and popular open source operating systems (e.g., Debian) (right graphic below)⁸ have similarly grown rapidly (Figure 5).

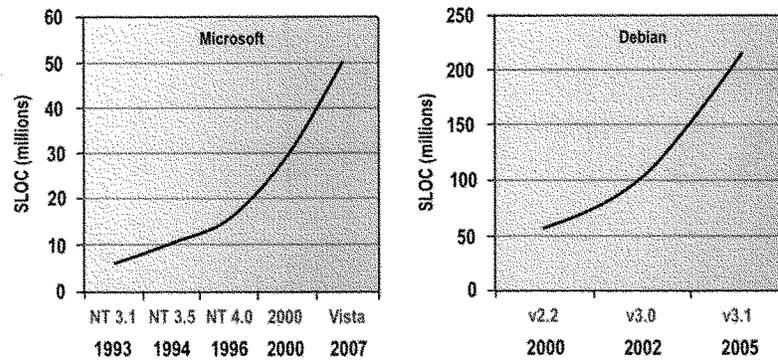


Figure 5. Source Lines of Code (SLOC) for Windows and Debian Operating Systems

Figure 5 also implies that DOD's total life cycle expenditures for software maintenance could grow, perhaps at a similarly exponential rate. Even more interesting, is that annual cost of maintaining the Department's software-enabled capabilities could not only rise exponentially but, where the capability is enabled by open-source software, could increase by ten times the cost of similar

7. "How Many Lines of Code in Windows?" Knowing.NET, December 6, 2005. See also Richard MacManus. 28 March 2006. "Measuring Source Lines Of Code (SLOC)—there are bigger birds than Microsoft's albatross" <http://blogs.zdnet.com/web2explorer/?p=148>.

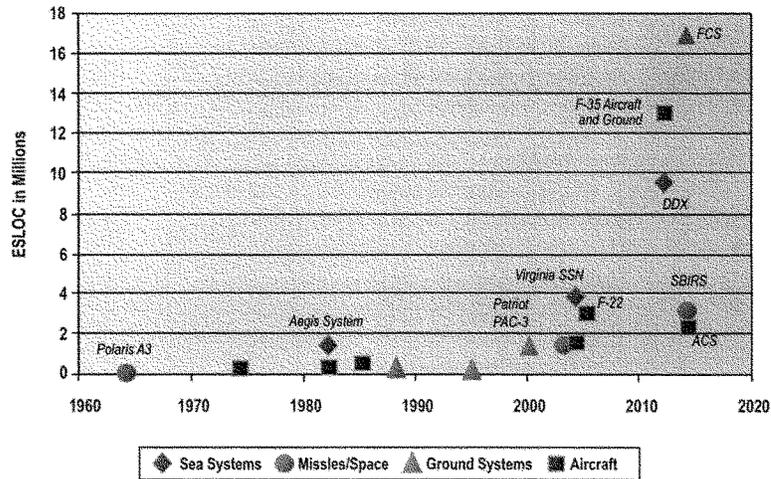
8. en.wikipedia.org/wiki/Source_lines_of_code

capability provided by the established and structured commercial software industry. This conclusion assumes that the cost of maintaining a single line of code is relatively constant over time and the maintenance cost (per SLOC) is the same for both commercial off-the-shelf and open source software. Clearly, the Department will have to develop a strategy to control this growth in a reasonable and practical way. That the majority of commercial code, such as for example Microsoft Windows, has grown exponentially while the cost has been nearly constant and has not tracked the lines-of-code metric, gives an even more compelling reason for DOD to develop standards and processes to use and acquire as much commercial-based code as possible.

Software has spread well beyond defense infrastructure into the very heart of weapon systems. For example, thousands of microprocessors, linear electric drive controllers, dynamic sensors, and millions of lines of sophisticated code enable the startling capabilities of the F-22 and Joint Strike Fighter, as well as quantum increases in the sensitivity achieved using pre-existing sensors. Several years ago a handheld grenade launcher was created with smart projectiles guided by 2,000 lines of code.⁹ Moreover, the software code base within mission systems is growing rapidly from generation to generation. The executable source lines of code (ESLOC) within weapon systems, such as missiles, ships, and aircraft have grown from a few thousand to tens of millions (Figure 6). For example, the 1.8 million LOC basis for the Navy's DDG 1000 is growing over 36 percent to 5 million LOC in the evolution to the Aegis 7.1R baseline.¹⁰ In addition, the FA-18 with approximately 10 million LOC is growing to over 15 million in the Joint Strike Fighter.

9. "Defense IT Official Says Talk on Software Quality is Cheap," *Government Computer News*, May 7, 2001 (mobile.gcn.com/articles/vol20_no10a/4167-1.html).

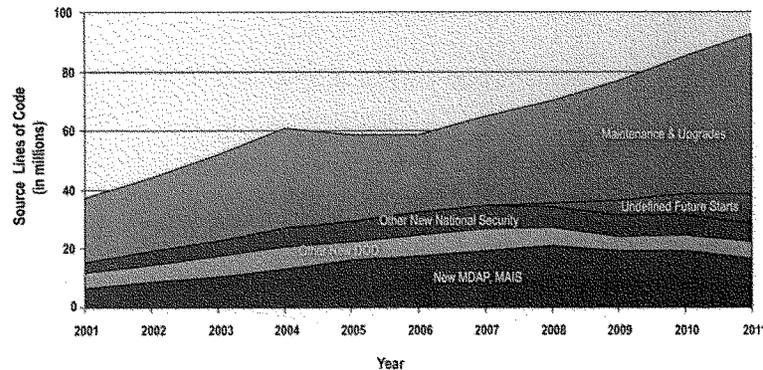
10. *Software Intensive Systems*, July 2006, Naval Research Advisory Committee Report, NRAC 06-03.



Sources: CARD Data, SEI, CSIS Analysis

Figure 6. Executable Source Lines of Code within Classic Weapon Systems

Because threats and capabilities change over time, it is expected that the Department's systems will require a continuing series of upgrades and technology refreshment. These costs can be substantial. The growth of SLOC for new MDAP and MAIS systems, and the SLOC for systems maintenance and upgrades are one example. Figure 7 depicts how code required for sustainment matches or exceeds those for new development. The figure also suggests that out-year budgets required to maintain and upgrade existing code will be substantial. The task force believes this to be a realistic projection for the tightly coupled code, which inhabits most existing DOD systems. However, this trend may not be inevitable. Open architectures, open standards, and service-oriented architectures, because of their mobile nature, appear to have the potential to dampen the projected rise in the cost of maintaining and upgrading software-based capabilities.



Source: CARD data, Federal Procurement Database System, QSM, CSIS Analysis

Figure 7. Estimated Source Lines of Code for the National Security Community

ESLOC is a valuable and intuitive measure that is correlated with the number of people required to build, use, and maintain software systems.¹¹ However, dimensions beyond size can significantly increase the complexity of IT systems. For example, Boehm and Lane (2006)¹² describe how software intensive systems of systems (SISOS) “integrate multiple, independently developed systems” and “are very large, dynamically evolving, and unprecedented with emergent requirements and behaviors, and complex socio-technical issues to address.” SISOS are characterized by 10–100 million LOC; 30–300 external interfaces; 2–200 suppliers; 6–12 hierarchical levels of suppliers (primes and subs) and 20–200 coordination groups (or integrated product teams).

Boehm and Lane argue for a risk-driven spiral development model that addresses the acquisition challenges of many systems, many supplier levels, and many increments where rapid fielding, high assurance, and evolution are essential for success. They point out successful continuous independent verification and validation practices found in the continuous build practices at Microsoft¹³ and in

11. Booch, G., 2008. “Measuring Architectural Complexity.” *IEEE Software*.

12. Boehm, B. and Lane, J. A. May, 2006. “21st Century Processes for Acquiring 21st Century Software-Intensive Systems of Systems.” *CrossTalk: The Journal of Defense Software Engineering*. www.stsc.hill.af.mil/crosstalk/2006/05/0605boehmlane.html.

13. Cusumano, M., and R. Selby. *Microsoft Secrets*. Harper Collins, 1996.

agile methods¹⁴ as well as the use of anchor point milestones and evolutionary development in the Rational Unified Process.¹⁵

Vulnerability

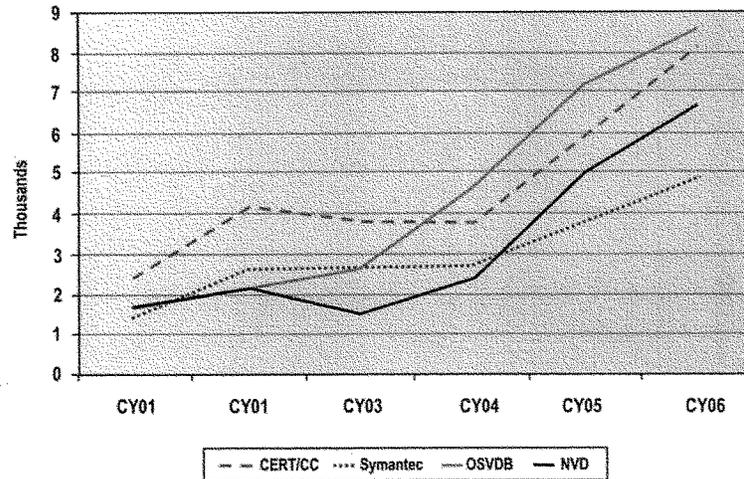
Increasing amounts of FSLOC increases the likelihood of vulnerabilities. The Common Vulnerabilities Enumeration (CVE) site (cve.mitre.org) in October of 2008 was reporting 19 new vulnerabilities each day. The number of vulnerabilities captured in the National Vulnerability Database (nvd.nist.gov), which incorporates CVE, has risen nearly four-fold from a yearly rate of 1,700 in 2001 to 6,700 in 2007. As of October 2008, there were over 33,337 CVE vulnerabilities in the data base.

The latest available data from four vulnerability sources confirms the exponential growth trend in recent years (Figure 8). In short, more software means more vulnerability. Adversaries understand this. Thus, not only are vulnerabilities increasing, the threat is increasing as well. It is also more diverse, ranging from capable state actors to small, independent, non-state rogue actors, all of which can produce enormous consequences. According to one source, attack volume has increased from 50 to 5,000 per week. Adversary attacks have also increased in sophistication (e.g., from general phishing to individualized spear phishing based on intelligence). Similarly, the number of viruses rose from approximately 20,000 in 1998, to 50,000 by 2000, to over 1 million in 2008.

This growth in vulnerabilities cannot be ignored in defense systems. In reality, vulnerabilities cannot be completely eliminated; therefore it must be assumed that some vulnerability will always exist. *DOD must develop tactics, techniques, and procedures, and concepts of operations to operate with degraded systems.* Continual tests to validate system and subsystem integrity must also be performed.

14. Beck, K. *Extreme Programming Explained*. Addison-Wesley, 1999.

15. Rational, Inc. *Driving Better Business With Better Software Economics*. Rational Software Corp. 2001.



Source: Computer Emergency Response Team Coordination Center (CERT/CC), Symantec Vulnerability Database, Open-Source Vulnerability Database (OSVDB), and National Vulnerability Database (NVD)

Figure 8. Correlated Upward Trends in Vulnerabilities

Cost

Another unfavorable trend is the cost of IT acquisitions. While hardware costs tend to follow a predictable trend, pricing software is challenging for many reasons. Though duplication cost is low, service life is difficult to predict. Commercial software pricing is challenging, for example, because cost can be based on upgrades, stand-alones, or suites. In a study of operating system unit costs, while the average price grew about one percent a year in the 1990s, when normalized for the functionality actually provided (which typically increases over the years), unit costs actually declined between 6 and 16 percent per year.¹⁶ Yet commercial software has become such a large cost and valuable investment that the Financial Accounting Standards Board no longer considers it an intangible

16. National Academies Press. 2006. *Measuring and Sustaining the New Economy*, Figure 5, p. 19. www.nap.edu/catalog/11587.html.

asset but rather a fixed asset (like property, plant, and equipment). Since 1998, even the design phase of software development can be capitalized.

The Government Accountability Office (GAO) reports that 48 percent of the federal government's major IT projects have been rebaselined at least twice.¹⁷ A 2008 RAND study of cost growth in 35 weapon programs found that development cost growth is driven equally by cost-estimating errors and requirements growth, which account for almost two-thirds the total cost growth.¹⁸

Acquisitions may have different cost curves during their life cycles. A complex, advanced weapon system program with a very long development cycle and few production items could anticipate the bulk of the costs to be up front. However, for a weapon system program with a short development cycle and many production items (e.g., MRAP), the bulk of the costs would occur after Milestone C. For IT acquisitions, which are not development-intensive, costs are likely to be primarily after Milestone C, whereas for complex development systems with few production items, the bulk of the costs will end up being up front.

Up-front rigorous capability (requirements) definition and systems engineering has been demonstrated to be inversely correlated with cost growth. As illustrated across a range of NASA programs, performance improves when a significant fraction (up to 12 percent) of program cost is for effective systems architecture and engineering (Figure 9).¹⁹ Acquisition experts cite flexibility to make informed trade-off decisions at the program level, as well as concentrating on managably sized increments that deliver capabilities in shorter time frames, as essential elements of this success. Unfortunately, the initial requirements definition and trade-off phase is rarely performed with sufficient rigor.

17. *OMB and Agencies Need to Improve Planning, Management, and Oversight of Projects Totaling Billions of Dollars*. July 2008. GAO-08-1051T. Washington, D.C.: Government Accountability Office.

18. Joseph G. Bolton, Robert S. Leonard, Mark V. Arena, Obaid Younossi, and Jerry M. Sollinger. 2008. *Sources of Weapon System Cost Growth: Analysis of 35 Major Defense Acquisition Programs*. Santa Monica, Calif: RAND Corporation. www.rand.org/pubs/monographs/2008/RAND_MG670.pdf.

19. Briefing on Alternative Acquisition Model, OSD (NII)/DOD CIO, DASD for C3ISR and IT Acquisition, Irvine, Calif., August 2008.

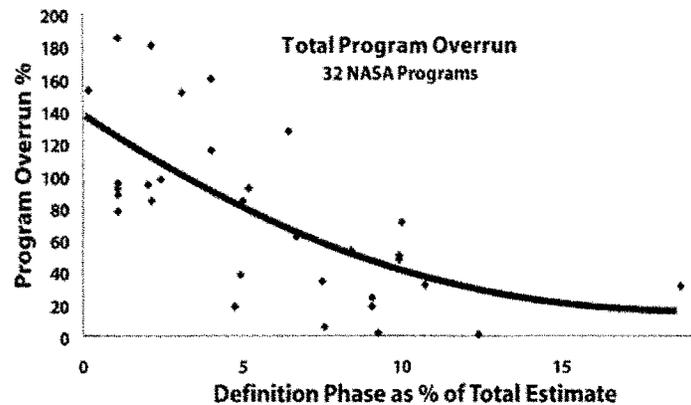


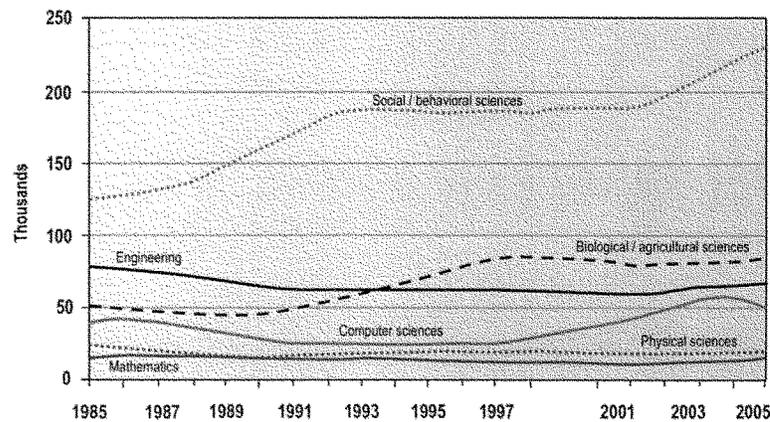
Figure 9. Rigorous Upfront Engineering Reduces Program Cost Overrun

Human Resources

The long-term supply of U.S. science and engineering students is worrisome and arguably a national security concern. Over the past decade, undergraduate engineering degrees in the United States, United Kingdom, Germany, and Japan have remained flat whereas South Korea's have risen significantly and China's have grown exponentially. While one can argue western schools are higher quality, quantity has a quality all its own. The number of doctorate degrees earned in China is growing exponentially—at a rate that could surpass the U.S. lead in annual production of doctorates in only a few years. Other countries, such as Germany, United Kingdom, Japan, and South Korea seem to be increasing the rate of their graduation of doctoral students at about the same rate as the United States. At the same time, the number of foreign students earning technical doctoral degrees in the United States has, for decades, been very high relative to U.S. citizens.

Not only is the raw amount of U.S. students at a global competitive disadvantage, but there is a growing gap between degrees earned in the social behavioral sciences as compared to engineering, computer science, and mathematics—one that favors social and behavioral science degrees (Figure 10). The Computing Research Association reports that after seven years of decline, the number of new computer science majors in 2007 was half of what it was in

2000.²⁰ Driven by declines in enrollment, the median graduates per computer science department dropped from 70 to 40 between 2004 and 2007.



Source: webcaspar.nsf.gov

Figure 10. Granted Bachelor Degrees in the United States

This decline in U.S. software talent is occurring in the face of increased demand. The gap between degreed professionals and job openings is growing, most notably in mathematics and computer science where only half the annual job openings can be satisfied by newly degreed students (Figure 11).²¹ The latest data in the National Employment Matrix from the Bureau of Labor Statistics project 324,000 new computer software engineering jobs over the 2006 to 2016 period.²² This 38 percent increase is much faster than the average for all occupations and one of the largest employment increases of any occupation.

20. www.cra.org/wp/index.php?p=139

21. As reported by Computer Research Association. www.cra.org/govaffairs/blog/projected_job_openings.pdf

22. www.bls.gov/oco/ocos267.htm#outlook

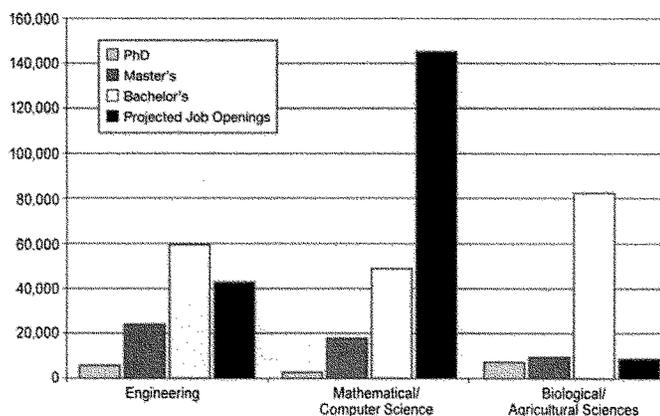


Figure 11. Annual Degrees and Job Openings, 2002–2012

To make matters worse, qualified IT systems designers, architects, and acquirers can take years to cultivate. Unfortunately, between 2002–2005, DOD experienced decreases in program managers (-5 percent), production engineers (-12 percent) and financial managers (-20 percent), whereas the test and evaluation workforce grew by 40 percent.²³ The result of the decline in experienced personnel, whether in government or industry, can be expensive rework, further increasing costs and exacerbating workforce challenges. (One GAO report cites as much as 40 percent rework in software acquisitions.)

Foreign Supply

At the same time that the supply of IT talent in the United States is declining, foreign sources of supply are rapidly growing, with notable increases in offshoring to India, Russia, and China. According to a 2007/2008 survey of 418 corporations, software and product development are the highest offshored functions, with over 70 percent of the software industry now offshoring.²⁴ Over the past ten years, India has

23. *Defense Acquisition Performance Assessment Report*, January 2006.

24. Lewin, A. and Heijmen, A. 2008. *Offshoring: An Intermediary Step to New Transformational Global Capabilities—Findings from the 2007-08 Offshoring Research Survey*. The Conference Board Strategic Outsourcing Webcast. Achieving the Next Evolution of Success. The survey also found that over 50 percent of companies are offshoring software development and over 30 percent new product development.

declined as the leading offshore product developer and many new specialized locations are emerging (e.g., the Middle East, Western and Eastern Europe, Latin America, Mexico, the Philippines and Russia) making supply chain analysis and risk mitigation increasingly distributed and more difficult.

Offshoring motivations are strong and include not only cost savings but growth, competitiveness, access to expertise, flexibility, and increasing speed-to-market. Service providers now aim to build capabilities to provide end-to-end business process re-engineering. Justifiably, there is increasing concern about our ability as a nation to ensure we can buy “trusted” components for our national security systems from an increasingly offshore supply chain. In 2007, a Defense Science Board task force that studied foreign influence on DOD software recommended that an intelligent risk management process is essential to ensuring a trusted supply chain, mitigate malicious attacks, enable efficient responses, and maintain trustworthiness in the software that support DOD’s critical missions.²⁵

Time

In addition to the challenge brought by the shortage of human expertise, the Department also faces the tyranny of time. Time scales are decreasing in two aspects. First, the pace of technology change puts pressure on acquisition time lines in order to ensure relevancy. Second, missions have evolved and are requiring increasingly more rapid response times. Conventional warfare decision cycles have shortened from days or hours to, in some cases, seconds. For example, cyber attacks on IT systems used to be lengthy, planned-out attacks, but now automated scanning, analysis, and global sharing of attack vectors enable attack cycles to occur in minutes and sometimes seconds. Unfortunately, the overall portfolio of DOD IT programs has experienced a 21-month delay in delivering initial operational capability to the war fighter, and 12 percent are more than four years late.²⁶

25. *Defense Science Board Task Force on Mission Impact of Foreign Influence on DOD Software*, 2007, Under Secretary of Defense for Acquisition, Technology, and Logistics. The task force also made recommendations in areas of procurements, intelligence, quality and security assurance, acquisition, research and development, and the national agenda. See also *Defense Science Board Task Force on High Performance Microchip Supply*, February 2005.

26. GAO-08-782, “Better Weapon Program Outcomes Require Discipline, Accountability, and Fundamental Changes in the Acquisition Environment,” June 3, 2008, p. 5.

Implications for Enterprise IT Acquisition

To be successful, future acquisition strategies must recognize and deal with the challenges outlined in this chapter. In particular, the growing dependence on information systems and commercial technology will mean increased

- cost whenever unique “requirements” are specified
- dependence on management of software-intensive programs
- reliance on a shared, common information infrastructure
- vulnerability with added functionality

Provisioning an information infrastructure of the scale, security, reliability, and functionality suitable for the Department of Defense is a challenge to software system design. Two principles, however, are proving effective in large-scale commercial situations:

- **Creation of a centralized governance (not program management) authority for enterprise oversight.** A successful information infrastructure—even one of the complexity of DOD’s—must have a central locus for conceptual integrity. This locus should be disassociated from implementation, but have implementation visibility to identify non-compliant initiatives and problems with the conceptual framework.
- **Creation of an enterprise concept built of elements loosely coupled.** A commercial consensus is emerging regarding an approach to large-scale enterprise implementations that takes advantage of the agility afforded by incremental development approaches, economies of software reuse, and ubiquity of web-based commercial products. This approach (service-oriented architecture) is a methodology supported by an evolving set of open commercial standards. Loose data coupling, as exemplified by Cursor on Target, should also be practiced where appropriate.

As with other large-system implementations, SOA partitions function using structured, well defined interfaces. Notably, the partitions are created in a way to support automated discovery, use, and reconfiguration over time. SOA also has special challenges for DOD. Standards, especially in the security domain, are still evolving. High-performance applications may not be well suited for the SOA approach. Nonetheless, the SOA approach, under the guidance of a centralized oversight authority, offers a way to move forward with incremental acquisitions while doing so in alignment with the Department’s strategic goals.

Chapter 3. A Framework for Information Technology Acquisition

The term “information technology” covers a broad range of technologies, war fighting domains, mission applications, and “customers.” For clarity we repeat the definition of IT, stated earlier, as any system or subsystem of hardware and/or software whose purpose is acquiring, processing, storing or communicating information or data. To manage this disparate set of uses and users, the task force found it useful to create an IT acquisition framework (Figure 12). The framework offered a means by which to identify substantive areas of commonality and differences between various uses and users, and to gain greater insight into policy and procedural issues affecting IT acquisition. Like any framework, it is an imperfect model of reality, but it is useful in addressing the issues at hand.

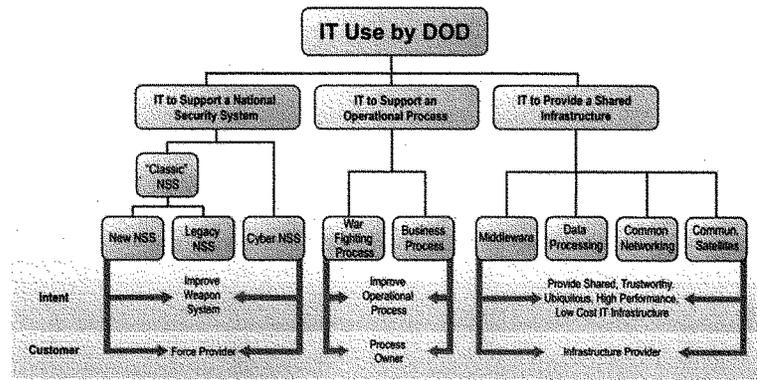


Figure 12. An Information Technology Acquisition Framework

The framework identifies three IT domains that are defined by the mission families in which the IT is used and the eventual customers:

- IT supporting national security systems
- IT supporting operational processes
- IT providing a shared infrastructure for either of the above

IT Supporting National Security Systems

National security systems (NSS) are war fighting systems, such as ships, tanks, missiles, satellites, and planes. IT is embedded within the system so that the end-product achieves its overall purpose. “Customers” of such programs are ultimately users, the war fighters, who obtain their equipment through the force providers. Examples of embedded IT applications include fire control, guidance, communications, and sensing. (For purposes of this study, we also include special networking capabilities that connect NSSs to a broader network.)

The use of embedded IT is becoming pervasive. More and more war fighting system functionality is being determined by embedded software instead of hardware, and many of the issues associated with acquiring and maintaining pure IT systems are applicable to embedded IT. In particular, the large disparity between the rapid turnover of IT and the much longer weapons systems development times is an especially important issue that must be managed.

For IT supporting national security systems, it is necessary to differentiate between new and legacy (existing) systems. IT as an embedded part of a “new” war fighting system (e.g., the radar for the proposed CGX cruiser, or fire control for the Airborne Laser), will have undergone a trade-off process to determine the best approach to meeting the program requirements. This process determines whether a requirement will be met by an approach that uses IT or an alternative that does not. In fact there are many design trade-offs in new national security systems for partitioning the functions and interoperability of embedded IT systems and subsystems, while assuring interoperability and network compatibility with the larger enterprise. At the same time there are likely to be areas of needed technology development requiring advances in science and engineering that have little or nothing to do with IT—such as increased speed or stealth. This later scientific and engineering technology development should not be confused with the traditional jargon of the IT community that defines technology development nearly interchangeably with software development and hardware integration.

IT that is an embedded part of an existing, legacy war fighting system is usually changed in order to provide upgraded or new capabilities. Examples include a fire control upgrade for the Aegis system to address national ballistic missile defense needs, the Acoustic Rapid COTS Insertion program for submarine SONAR improvements, and Link 16 upgrades. In many such cases, key architectural trade-offs will have already been made in the original acquisition program and changes to the system and its information technology are often constrained by those original

program decisions. The task force believes that appropriate acquisition policies for legacy NSS will have more in common with policies for operational processes and much of the infrastructure than it will for policies covering new NSS—a fact that motivated the differentiation in categories.

There are, of course, gray areas. There may be next-generation systems that require such extensive changes that the original architectural trade-offs have to be revisited to allow substantive changes to underlying IT and hardware choices. In this case, the acquisition of a “legacy system” has more characteristics of a new acquisition program than a legacy one.

In Figure 12, these two cases—new and legacy national security systems—were identified as “Classic NSS.” To account for the emergence of defense to cyber attacks, a cyber NSS is a system for the cyber domain, the customer of which is a force provider. In this way, it is similar to a conventional NSS such as a missile, but has many of the characteristics of a conventional IT system—workstations, servers, and networks. Therefore, “Cyber NSS” is in the eyes of an acquirer, a conventional IT system for the special purpose of defense of the cyber domain and delivered for use to force providers.

IT Supporting Operational Processes

Conventional IT systems (workstations, servers, and networks) are used to support operational processes in war fighting, much as they are used to support operational processes commercially. Two classes of such processes are of interest to DOD: war fighting processes and DOD business processes. In the first case, IT is developed as a tool set for the processes used to support war fighting operations (e.g., the Tomahawk Planning System, command and control systems, logistics systems, an intelligence analyst’s workstation). In the second case, IT is developed as a tool set for processes used to support DOD business operations (e.g., payroll, purchasing, finance, TRICARE medical operations). The customer, in either case, is the “process owner” and the purpose of using IT is to make the end-process more effective.

From a war fighting perspective, these two cases are very different, but from an IT acquisition perspective, they are very similar. The acquisition program needs to balance and ensure consistency between the process being followed (tactics, techniques, and procedures), the tools being built (IT systems), and the training and capabilities of the people who will use these tools within these

processes. This need for balance holds true regardless of whether one is dealing with nuclear command and control or with staff hiring.

IT Providing a Shared Infrastructure

In a net-centric world, no deployed IT systems are islands unto themselves—they exist as part of a shared IT environment. They are usually interconnected to several others through a network, sometimes a global network that provides global interconnection. More and more, these IT systems are being constructed of common elements. Computing platforms have become commodities and are common to all applications except the most unique. A few operating systems have become ubiquitous. Commonly used middleware is more prevalent than ever before. Certain applications have become de facto standards even in the most demanding situations (e.g., the use of Power Point in command and control).

IT that provides a shared infrastructure is acting as a “utility” to various national security systems and operational processes. These utilities are at the processing, networking, and middleware levels.

- Data processing utilities are services that provide general purpose data processing capabilities (e.g., DISA data centers, servers, workstations).
- Common networking utilities are interconnection services (e.g., fiber networks, routers, long haul Internet-protocol networking services, voice-over-Internet protocol products and services).
- Middleware utilities are services that support higher level applications (e.g., directory services, security services, storage services, message services).

The intent of these services is to provide shared, trustworthy, ubiquitous, high performance, low-cost IT capabilities that allow both national security and operational process systems to fulfill their goals.

As will be observed later in this report, acquisition for shared infrastructure IT systems, with one major exception, has more in common with acquisition for operational process IT systems and legacy NSS IT systems than it does for new NSS IT systems. The major exception deals with IT for communication satellites—that is, those satellites developed to provide long-haul communications (e.g., MUOS or MILSTAR). For this exception, acquiring these systems requires the same trade-off analysis, architectural decisions, and perhaps technology development that new national security IT systems require, and the realization process used to acquire them will have to be similar.

Chapter 4. Existing Defense Acquisition Process

While the task force was underway, the defense acquisition process was being actively reviewed, with the expectation that a new process would be approved by the time of the report's release. Thus, this chapter provides an overview of the process that existed during the task force deliberations, as well as the revised process, implemented in December 2008, and the improvements it was intended to bring forth.

Existing Acquisition Process

The defense acquisition process, prior to December 2008, was approved in 2003 (Figure 13). Its central purpose is to provide a simplified and flexible management framework for translating approved capability needs and technology opportunities into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and automated information systems.

The process includes five activity phases starting with concept refinement and ending with production and deployment, and operational support. The key actors are the program manager and the milestone decision authority (MDA) who are given broad authority to exercise discretion and prudent business judgment to structure a tailored, responsive, and innovative program.

Multiple milestones and decision points throughout the process permit a program manager to report progress and the MDA to provide permission to proceed to subsequent phases. MDAs are given the flexibility to tailor procedures to achieve cost, schedule, and performance goals, and may authorize entry into the acquisition management process at any point (milestone) consistent with phase-specific entrance criteria and statutory requirements. Progress depends on obtaining sufficient knowledge to continue to the next phase of development. Evolutionary acquisition, or the division of capability into smaller, more executable increments, is DOD's preferred strategy for rapid acquisition of capability.

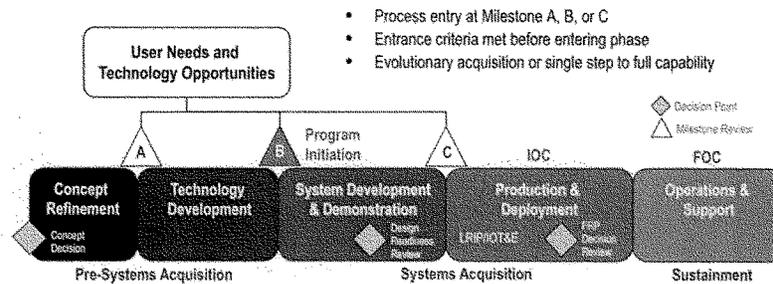


Figure 13. Prior Defense Acquisition Process

This process was designed to accommodate the needs of all programs including information technology. On most occasions, MDAs and program managers have used the inherent flexibility of the acquisition process to proceed directly to Milestone B, or enter into the System Development and Demonstration (SDD) phase, the point where programs are typically initiated. In many cases, this truncated process does not produce desirable results. In short, the deliberate and thoughtful activity of the several phases that precede SDD is either not accomplished in a substantive way or is compressed into the period immediately preceding Milestone B.

The result is that program cost, schedule, and performance may be inadequately informed by the requirements/design trade-offs that are intended to occur during earlier phases. Further, system maturity and compatibility may not have been adequately demonstrated prior to program initiation. Consequently, programs may proceed to development with additional risk and program outcomes are less predictable. Perhaps even more important, the proposed capability may not have been adequately tested against national security objectives to assure that the program supports the most pressing military missions of the Department. Given that the Services are the providers of materiel, programs sometimes reflect Service, rather than Department, priorities.

The New Defense Acquisition Process

A new defense acquisition process was approved in December 2008 (Figure 14). The new process remains generally applicable to IT programs and sustains the former emphasis on process flexibility and evolutionary acquisition. While

maintaining many of the same structural characteristics of the earlier process, it introduces some important policy changes intended to improve process discipline, program stability, and program outcomes.

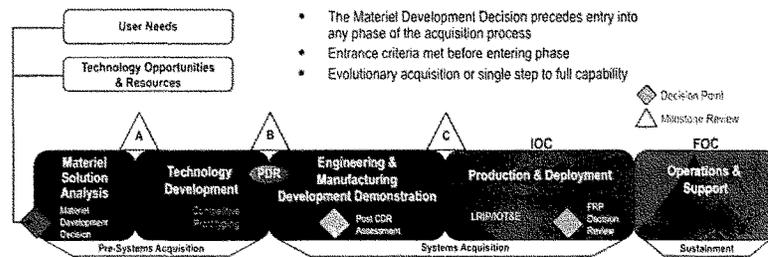


Figure 14. New Defense Acquisition Process

Policy changes embedded in the new process include the following:

- All programs will proceed through a formal acquisition process entry point, the Materiel Development Decision (MDD). Programs will no longer immediately proceed to Milestone B. Consequently, the vast majority of programs will benefit from the improved conception and technical maturity resulting from the early phases of development.
- Programs requiring technology development will conduct competitive prototyping at the system or sub-system level, when appropriate, to ensure that technologies have been demonstrated in a relevant environment and, consequently, key risks have been retired before programs are initiated.
- Where consistent with the strategy for the Technology Development Phase, preliminary designs will be prepared to ensure that requirements are well understood and cost estimates well informed.
- The Engineering and Manufacturing Phase has been redesigned to place additional emphasis on systems engineering and manufacturing readiness.
- Configuration Steering Boards have been established to ensure that requirements changes/creep, a traditional contributor to increased cost and extended schedules, are not casually approved.

While the task force agrees that these are substantive changes with potential to improve the acquisition process, more can be done to tailor the acquisition process to the unique attributes of information technology, as will be discussed in the following two chapters.

Oversight Responsibility

Oversight is a necessary and important part of the defense acquisition process, which employs a layered approach to oversight based on the level of investment (Figure 15). All programs are conceived and designed at the component level consistent with formally approved requirements. Most programs are reviewed at the same level by designated component milestone decision authorities (MDAs), typically the component acquisition executive (CAE) or a program executive officer (a flag officer or SES). The most significant investments, programs categorized as major automated information systems (MAIS) or major defense acquisition programs (MDAPs), receive additional review within the Office of the Secretary of Defense (OSD).

At the OSD level, major systems (both weapon systems and automated information systems) are initially assessed by specialized review teams called Overarching Integrated Product Teams (OIPTs) staffed with executive-level subject matter experts (Table 1). (The Investment Review Board (IRB) serves the same purpose for Business Transformation MAIS.) The ASD (NII) OIPT and the Business Transformation Agency IRB are focused on information systems, with the latter focused specifically on IT business systems. Another OIPT is principally focused on weapon systems. These groups review programs to ensure they are well planned and compliant with statute and regulation. Their findings and recommendations are reported to the milestone decision authority.

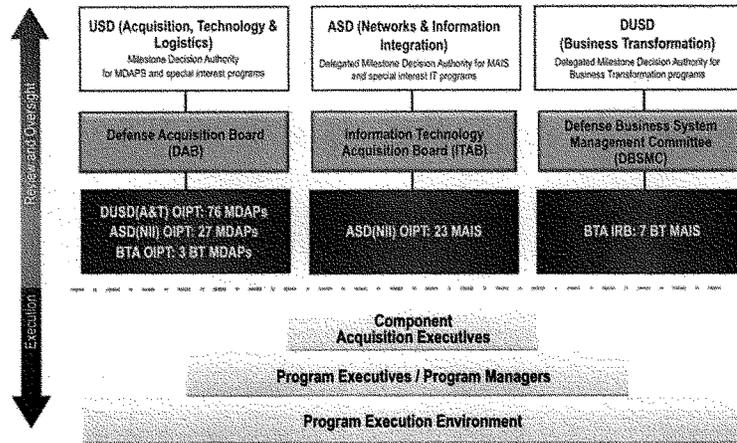


Figure 15. OSD Acquisition Oversight Responsibility

The USD (AT&L) is the milestone decision authority for major defense acquisition programs and for MAIS that achieve the same funding threshold. The ASD (NII), with authority delegated by USD (AT&L), is the milestone decision authority for a portfolio of MAIS programs and the Deputy Under Secretary of Defense for Business Transformation, also with delegated authority, is the milestone decision authority for MAIS business systems. Each of the three MDAs is advised by senior executive boards: the Defense Acquisition Board, which covers weapon systems; the Information Technology Acquisition Board, which covers major automated information systems; and the Defense Business Systems Management Committee, covering MAIS business systems. Each milestone decision authority has approval authority over assigned programs.

Programs are reviewed and approved by the milestone decision authority at key decision points in the acquisition business process to ensure they are being conceived, designed, and executed consistent with sound business practices and the approved acquisition program baseline (cost, schedule, and performance objectives). Programs are executed at the component level under the direct supervision of the component acquisition executive, program executive officers, and the program manager.

Table 1. Acquisition Category Designation

Acquisition Category	Reason for ACAT Designation	Decision Authority
ACAT I	<ul style="list-style-type: none"> • MDAP (section 2430 of Title 10, United States Code) • Dollar value: estimated by the USD(AT&L) to require an eventual total expenditure for research, development, test and evaluation (RDT&E) of more than \$365 million in fiscal year (FY) 2000 constant dollars or, for procurement, of more than \$2.190 billion in FY 2000 constant dollars • MDA designation • MDA designation as special interest 	<ul style="list-style-type: none"> • ACAT ID: USD(AT&L) • ACAT IC: Head of the DOD Component or, if delegated, the CAE (not further delegable)
ACAT IA	<ul style="list-style-type: none"> • MAIS (Chapter 144A of Title 10 of U.S.C.): A DOD acquisition program for an Automated Information System (either as a product or a service) that is either: • Designated by the MDA as a MAIS; or • Estimated to exceed: \$32 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred in any single fiscal year; or • \$126 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or • \$378 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system. • MDA designation as special interest 	<ul style="list-style-type: none"> • ACAT IAM: USD(AT&L) or designee • ACAT IAC: Head of the DOD Component or, if delegated, the CAE (not further delegable)
ACAT II	<ul style="list-style-type: none"> • Does not meet criteria for ACAT I • Major system • Dollar value: estimated by the DOD component head to require an eventual total expenditure for RDT&E of more than \$140 million in FY 2000 constant dollars, or for procurement of more than \$660 million in FY 2000 constant dollars (section 2302d of Title 10, United States Code) • MDA designation (paragraph (5) of section 2302 of Title 10, United States Code) 	<ul style="list-style-type: none"> • CAE or the individual designated by the CAE
ACAT III	<ul style="list-style-type: none"> • Does not meet criteria for ACAT II or above • AIS that is not a MAIS 	<ul style="list-style-type: none"> • Designated by the CAE

Chapter 5. IT Acquisition Challenges and Issues

As the previous chapter described, information technology is currently procured using the same acquisition system as is used for major hardware systems. The acquisition model most often employed is the familiar “waterfall” development model in which well-defined increments of capability or technology are designed, developed, and fielded in a pre-specified order. The “flow” of releases is sequential and deviations from the approved sequence are cause for a new baseline for the program (or in extreme cases cancellation). Since a new baseline generally triggers a complete top-to-bottom review of the program, delays are inherent and often approvals at each step up the acquisition approval chain become more difficult to obtain. The result is usually an increase in the time required to deliver the increment(s) and the program.

In his recent *Foreign Affairs* article, Secretary of Defense Robert Gates highlighted trends in today’s acquisition process with platforms growing even more “baroque.”²⁷ He questioned the necessity to go outside the normal bureaucratic process to develop technologies that will counter improvised explosive devices, build Mine Resistant Ambush Protected (MRAP) vehicles, and quickly expand U.S. ISR capabilities. In short, he questioned the efficacy of the current acquisition process, given the apparent need to bypass existing institutions and procedures to rapidly field needed capabilities to protect U.S. troops on the battlefield. The Secretary issued a call to the defense establishment to think hard about the current acquisition paradigm—a procurement process that seeks a 99 percent solution over a period of years, when today’s missions require solutions over a period of months or even weeks.

Where technologies or requirements can be developed and delivered over a relatively large timeframe (years), the traditional waterfall acquisition model can deliver acceptable results—war fighters get needed capabilities in time to counter or deter the threat. However, when that timeframe is small (hours, days, or months), the deliberate, sequential nature of the waterfall model does not serve

27. Robert Gates. 2009. “A Balanced Strategy: Reprogramming the Pentagon for a New Age,” *Foreign Affairs*, January/February.

DOD well. Information technologies reside in a domain where change occurs in small timeframes, both for technology and for the ability of adversaries to procure, adapt, and employ the technologies.

An analysis of 32 major automated information system acquisitions, conducted by the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII)), calculated that the average time to deliver an initial program capability is 91 months (Figure 16). Today's "big bang" approach used in the acquisition of IT begins with an analysis phase followed by an equally long development phase that culminates in a single test and evaluation event. The average time between the start of a program's analysis phase (Analysis of Alternatives) to Milestone B (System Development and Demonstration)—is 43 months: 14 months to complete the analysis of alternatives (AoA) and 29 months to complete the economic analysis (EA). Likewise, it took an average of 48 months to deliver useful functionality from the Milestone B decision—40 months for development and an additional 5 months for operational test and evaluation

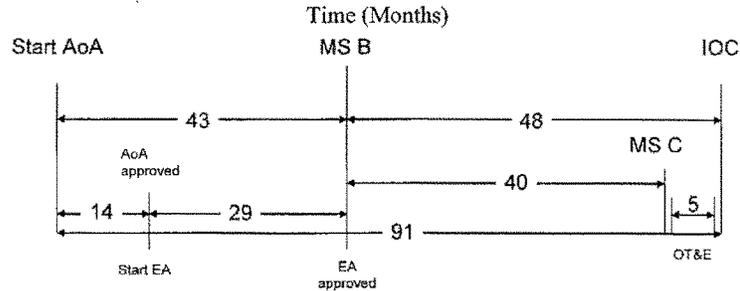


Figure 16. MAIS Acquisition Timeline

An advantage of current IT technologies (some would say a "complexity") not addressed within current DOD acquisition policies and procedures, is that the acquisition of IT does not necessarily require delivery of a "system" but instead may involve providing new services or capabilities, that may require only small investments to the supporting IT infrastructure. Given the current investments by commercial industries to invest in and deploy service-oriented

architectures, the task force expects that DOD and the Services will seek to adopt similar technologies. Without an acquisition process that accommodates, and takes advantage of, IT's rapid pace of change, future DOD acquisition officials will likely be frustrated in their efforts to equip the nation's war fighters and weapon systems with the needed information technologies.

Why the Process is “Broken”

With so many prior acquisition reform efforts to leverage, any novel approach for acquiring IT is unlikely to have meaningful impact unless it addresses the barriers that prevented prior reform efforts from taking root. Perhaps the two most important barriers to address are experienced proven leadership and incentives (or lack thereof) to alter the behavior of individuals and organizations. According to the Defense Acquisition Performance Assessment Panel, “... current governance structure does not promote program success—actually, programs advance in spite of the oversight process rather than because of it.” This sentiment was echoed by a defense agency director in characterizing IT acquisition as hampered by the oversight organizations with little “skin in the game.”

Many functional organizations (Comptroller, Programs Analysis and Evaluation (PA&E), Office of the Director, Defense Research and Engineering (DDR&E), and Operational Test and Evaluation (OT&E)) have assumed the responsibility to “stop” programs that are unable to fully satisfy their concerns. While these offices can bring value during program reviews, the task force believes that the nature of their involvement must be adapted in order for DOD to achieve rapid acquisition of information technologies.

Acquisition improvements can only be achieved if the program's overriding focus is performance and schedule and if decisions to proceed are made at regular intervals by the acquisition decision authority with full knowledge of the risks. This approach implies that the program manager is not obliged to obtain a “thumbs up” from each functional organization. The program manager is obliged to do all within his authority to mitigate risk but the overriding priority is to conduct the decision meeting in accordance with a desired schedule for availability of capability. Although program managers must provide the acquisition decision authority with the risks identified by the functional organizations, the milestone decision authority holds the full burden of accountability for accepting (or rejecting) program risk on behalf of the Department or Service. The intent is to set the schedule of decision points to

match the schedule for providing fielded capability, and prevent the ability of well-intentioned and necessary functional reviews to slow or inhibit the decision-making schedule. To that end these functional organizations should be involved early and continually to provide their support and insight to assure program success, rather than become a “log jam” at decision points.

The use of the Technology Readiness Assessment (TRA) illustrates this point. Instead of applying technology readiness levels (TRL) to guide fundamental advances in science and engineering underlying cyber infrastructure and leap-ahead technologies, DOD employs TRLs to assess interoperability, logistics considerations, information assurance, system engineering, and effectiveness considerations. Much of the confusion stems from the fact that TRAs were developed for a hardware model and not designed to address the maturity of IT systems for acquisitions.

In presentations to the task force, DOD officials highlighted that TRA evaluations for IT were breaking new ground and included first-ever assessments. It appeared unclear whether these efforts were focused toward evaluating maturity of salient IT criteria such as those defined by the American National Standards Institute, Institute of Electronic and Electrical Engineers, or The Open Group’s Architectural Framework standards. Also, TRA evaluations are the responsibility of, and approval authority by, the Deputy Under Secretary of Defense for Science and Technology (DUSD (S&T)), and TRA oversight is executed outside the typical OIPT and program office structure. Instead, oversight is conducted by DUSD (S&T) who works directly with the Science and Technology Executive in the DOD component or agency. This results in confusion and debate regarding roles and responsibilities among the other functional oversight organizations (e.g., Chief Information Officer; Director of Logistics and Material Readiness; Director of Systems and Software Engineering; or Director of Operational Test and Evaluation).

It is not uncommon for this confusion of responsibilities to lead to extended coordination cycles as witnessed by the Net Enabled Command Capability (NECC). With well over a year following the TRA’s original submission to the Office of the Secretary of Defense and three separate agency attempts, the document has yet to be approved despite the program’s use of standard commercial off-the-shelf (COTS) technologies. Unable to proceed forward, Congress removed \$119 million from the program budget, which was subsequently followed by removal of an additional \$270 million by OSD (PA&E). While we do not question that acquired software should be assessed to

assure it is ready and appropriate to insert into a DOD system, we question “stretching” the hardware rules to involve organizations and people that have little experience in IT development or acquisition.

This confusion is not limited to the TRA. The acquisition strategy for the Enhanced Polar System was in OSD coordination for over eight months before ultimately being rejected because the Air Force approval was more than three months old. These examples are two of many illustrating the lack of accountability built into the acquisition governance system, which establishes neither clear incentives for positive performance nor discipline for poor performance, with no systematic tracking of either.

Section 814 of the 2006 National Defense Authorization Act directed the Defense Acquisition University to review DOD acquisition structures and capabilities. This analysis revealed that DOD acquisition organizations are continuously evolving to address better mission focus and improved productivity; however, it did not result in improved acquisition outcomes. Today, there are four different OSD-level organizations involved in IT acquisition:

- Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, who serves as the milestone decision authority for the 23 MAIS programs
- Business Transformation Office, who serves as the MDA for seven Enterprise Resource Planning software-intensive acquisitions
- Director of Systems and Software Engineering, with responsibility focused primarily on embedded IT in major weapon systems
- Director of Space and Intelligence Capabilities Office, who leads the acquisition oversight for National Intelligence Agency programs including numerous major software-intensive acquisitions

The leadership and staff experience within these organizations vary significantly. Some leaders have recent industry or acquisition executive experience, while others have neither IT expertise nor relevant industry experience in either the leadership or staff. Likewise, it is not clear that these organizations are working together to achieve the spirit of the Clinger-Cohen Act (40 U.S.C. 11314), or serve with common focus toward achieving the five-year time-certain development imposed as part of the 2009 National Defense Authorization Act.

Recent wartime experiences highlight the importance of IT and the ability to fuse information from a broad range of sources outside DOD boundaries. Today, information derived from national intelligence is having a dramatic impact on the lethality of the nation's war fighting forces, and future operations will likely require access to even more national and international information. At the time of Goldwater-Nichols, the vast enabling capability inherent within IT was not apparent nor was the understanding of the impact of extending the edge of modern computing to effectively leverage such capabilities. Figure 17 characterizes the long-standing government weakness regarding information resource planning and decision-making where modernizations so often occur within organizations that continue to be challenged by the lack of an integrated "enterprise" philosophy.

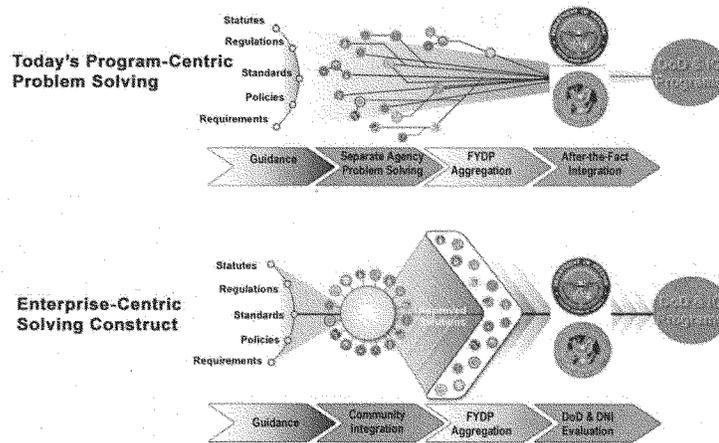


Figure 17. Effective Oversight Paradigm: Enterprise Level Decision Making

In addition to the need for more robust IT governance, DOD needs to better leverage the IT acquisition instruments and services of other federal agencies, to include better utilization of organizations such as the General Services Agency. Likewise, the Department needs to capitalize on the strides made in enhancing IT governance by better leveraging groups such as the CIO Executive Council in making investments, estimating costs, and enhancing the effective and efficient use of IT infrastructure. As the Department postures itself

for the future, the OSD acquisition oversight construct needs to be coherently linked to the larger CIO enterprise, with proper authorities to address organization-level decisions regarding information policy vision, architecture, strategy, and information assurance.

Maintaining a Knowledgeable and Experienced IT Acquisition Workforce

The number of programs having troubles associated with information technology, as reported by sources such as the GAO, suggests that the government is challenged in its ability to successfully manage the acquisition of these technologies. Anecdotal reports from industry suggest commercial companies face similar management challenges. Both government and industry have reported impending staffing difficulties due to the expected retirement of many in the current IT workforce and the small number of remaining and incoming personnel.

Given these demographics, the most often heard solutions are to streamline the processes and better train remaining and incoming personnel. The task force found these solutions to be reasonable, but perhaps insufficient.

In the years since Goldwater-Nichols, and sometimes due to “encouragement” by Congress, DOD has developed training and certification regimes for its acquisition workforce:

- The Defense Acquisition University was established to provide training and support to DOD’s acquisition workforce and program managers. In addition to courses on the acquisition of hardware-based technology, the university teaches courses on the management of software-intensive programs, including the processes pioneered by the Software Engineering Institute. All acquisition workforce members are required to complete a set course of instruction, and achieve a specified level of certification, before they can be permanently assigned to designated acquisition positions. For example, program executive officers, major program managers, and program managers must complete advanced courses in program management. Given the continually evolving character of best practices for IT systems and their management, it is imperative that the DOD CIO assure that these programs are current.
- Among DOD’s acquisition workforce are many individuals with degrees in disciplines such as computer science, systems engineering, electrical

engineering, engineering management, finance, and logistics. Many hold advanced degrees.

- Within the ranks of the uniformed military's core of acquisition professionals, advanced degrees and recurring tours in acquisition and/or engineering are prerequisites to advancement and selection to command.
- Within DOD and the Services, the selection (whether civilian or military) of a program executive officer, major program manager, or program manager (or the deputy to these positions) is, by directive, accomplished through a series of selection panels, committees, boards and officials—all charged with finding, recommending, and/or selecting the most qualified individual for the specific acquisition at hand.

Yet, in spite of the education requirements, certifications, and rigorous selection processes, the general impression remains that managing DOD's IT efforts should yield a better record of success. We must be clear that neither training nor education is a substitute for experience in successfully managing acquisition programs of increasing complexity. For that reason, the task force emphasizes proven experience, in addition to education and preparatory training, as the most important criteria for selecting individuals so that informed judgments based on experience can guide program decisions.

Many Other Studies Have Warned of IT Acquisition Challenges

Concerns regarding acquisition cycle time, flexibility, and efficiency have led to decades of studies and recommendations for improvement. Such acquisition reform studies have been on-going almost continuously since the original Goldwater-Nichols legislation was passed in 1986.

The Center for Strategic and International Studies sponsored several such acquisition reform studies including *Beyond Goldwater Nichols: Defense Reform Phase 1* and *Phase 2* in March 2004 and July 2005, respectively. These studies concluded that the U.S. national security apparatus requires significant reforms to meet the challenges of a new strategic era. As part of its transformational efforts, DOD must not only adapt to the post-cold war, post-9/11 security environment, but also cope with many "hidden failures" that, while not preventing operational success, stifle innovation and continue to squander critical resources in terms of time and money. It identified many organizational structures and processes initially constructed to maintain a cold war superpower

in the industrial age, but which are inappropriate for 21st century missions in an information age.

This sentiment was echoed by numerous leaders interviewed by this task force and characterized in the 2006 Quadrennial Defense Review (QDR) Report. In addition to an illustration of the gap in today's capability portfolio (Figure 18), the report noted, "as we emphasize agility, flexibility, responsiveness, and effectiveness in the operational forces, so too must the Department's organizations, processes and practices embody these characteristics if they are to support the joint war fighter and the Commander in Chief."

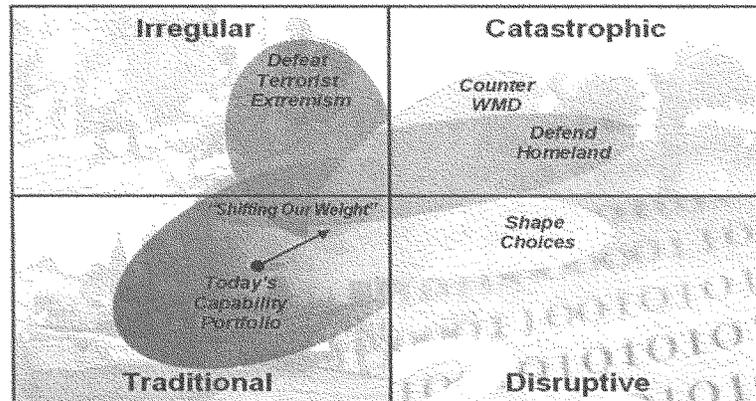
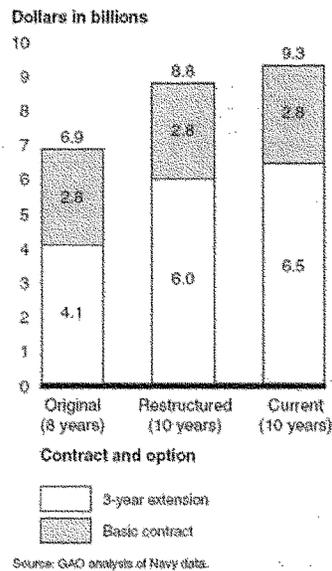


Figure 18. 2006 Quadrennial Defense Review Capabilities Portfolio

As mentioned earlier in this report, a RAND study on the cost growth of 35 weapon systems highlights that development cost growth is driven equally by cost estimating errors and requirements growth, which account for almost two-thirds of the total cost growth.²⁸ This conclusion also was shared by the GAO in its June 3, 2008 assessment that called for fundamental changes in the acquisition environment. It cited systemic problems at the strategic level resulting in a requirements and acquisition process that is neither agile enough to support

28. *Sources of Weapon System Cost Growth: Analysis of 35 Major Weapon Systems*, RAND Corporation, 2008. http://www.rand.org/pubs/monographs/2008/RAND_MG670.pdf

current operational needs nor able to effectively estimate the costs of such modernizations. Similar conclusions were likewise shared by several leaders interviewed by the task force who observed that the fundamental model used in the acquisition of IT capabilities is inappropriate. The 1990 Defense Science Board Task Force on Defense Software reported the need to move away from the waterfall model to an iterative model since approximately 90 percent of the time, the waterfall model results in late, over-budget, fragile and expensive-to-maintain software systems.



Cost overruns and schedule delays, which result in numerous audits and evaluations by independent government and industry organizations, also point to the need for a more streamlined IT acquisition system (Figure 19). A GAO review conducted in July 2008 concluded that 48 percent of the federal government's major IT projects have been re-baselined for several reasons, including changes in both project goals and funding. Of those projects, 51 percent were re-baselined at least twice.

Figure 19. Cost and Schedule Overruns in IT Programs

The Joint Tactical Radio System (JTRS) is one of many examples. Because of development and production delays, GAO reported that the military has more than doubled its spending on tactical radios from a planned \$3.2 billion to about \$8.3 billion over the past five years. Another example is the Navy Marine Corp Intranet (NMCI), reviewed by GAO in 2006. The NMCI program is a multiyear information technology services program. Its goals are to provide information superiority and foster innovation via interoperability and shared services. The

Navy awarded the NMCI services contract—currently valued at \$9.3 billion—to Electronic Data Systems (EDS) in October 2000.

The contract calls for EDS to replace thousands of independent networks, applications, and other hardware and software with a single, internal communications network (Intranet), and associated desktop, server, and infrastructure assets and services for Navy and Marine Corps customers. GAO's 2006 review of Navy data highlighted that NMCI has met only 3 of 20 performance targets (15 percent). It cited that five shipyard/air depots continue to rely on their legacy systems rather than NMCI. Officials at two of the sites stated that NMCI is hurting workforce productivity and users "reach back" to legacy systems because NMCI is slow, sometimes taking 45 minutes to open a document. Similar to JTRS, NMCI incurred significant cost growth from its original contract award with contract extensions, revisions, and engineering changes that also delayed capability.

Legislative Changes

Congress, in its oversight role, responds to the Department's acquisition shortfalls by adding more restrictive legislative mandates. The 2007 National Defense Authorization Act contained unprecedented mandates involving the acquisition of IT via Section 816 and Section 811. Section 816 was codified as 10 U.S.C. Chapter 144A. It defined the criteria for a MAIS program and, beginning in January 1, 2008, required annual reports to Congress containing the following:

- development schedule with major milestones
- implementation schedule including estimates of milestone dates, initial operational capability (IOC) and full operational capability
- estimates of development and life-cycle costs
- summary of key performance parameters

The statute also established Nunn-McCurdy-like reporting for MAIS programs by defining the initial report as the baseline for determining significant and critical changes. Any change in cost, schedule, or performance that exceeded predefined limits will be associated with a significant or critical change, triggering a report to Congress. Likewise, the statute required program managers to submit quarterly reports disclosing program variances to the senior Department official.

Section 811 implemented new time-certain development mandates for IT business systems. The statute requires that the milestone decision authority certify that the acquisition will achieve IOC in five years or less from Milestone A before granting approval. This requirement equally applies to all IT business system acquisitions regardless of their size. The only software-intensive programs excluded from this requirement are national security systems that directly support war fighter operations. If subsequent acquisition activities are unable to achieve IOC within five years, the system would be deemed to have undergone a critical change triggering reporting in accordance with 10 U.S.C. Chapter 144A.

In the 2009 National Defense Authorization Act (Section 812), Congress extended the reporting requirements defined in 10 U.S.C. Chapter 144A to include pre-MAIS programs. However, the value of this reporting is questionable since pre-MAIS programs typically do not have development or implementation schedules, cost estimates, or key performance parameters to baseline. Another mandate contained in Section 812 was the changes associated with time-certain developments. Instead of the 5-year requirement to achieve IOC from a program's Milestone A, the law changed the date from Milestone A to start "when funds for program are first obligated."

Chapter 6. A New Acquisition Process for Information Technology

While the task force recognizes DOD's efforts to improve the defense acquisition process, the planned changes do not go far enough to address the unique characteristics of information technology programs and the rapid timeframes within which such programs evolve. Implementing IT capability is a transformational endeavor; there are continually evolving best practices, processes, and organizational considerations that must be addressed. Thus, the task force proposes that DOD develop a new acquisition management model tailored to information technology.

The proposed model recognizes the unique aspects of information technology and provides more value-added activities, as compared to the current process. It includes enhanced stakeholder engagement and analytical rigor throughout the acquisition life cycle. Program reviews begin during the business case development phase and extend until full deployment of mission capability. In earlier phases of the acquisition, the quarterly program reviews should be calendar-based events (perhaps quarterly), while later phases should link such reviews with iterations or delivery of capability.

The success of this model is based on the following criteria:

- early and continual involvement of the user
- multiple, rapidly executed increments/releases of capability
 - well defined objectives but not over defined requirements for the initial increment
 - evolving requirements for subsequent increments/releases
 - mature technologies (often with short half-life that require periodic refresh)
- early, successive prototyping to support an evolutionary approach
- early operational release of capability from within an increment
- modular, open-systems approach—designed for ease of updates
- available full funding of initial increment(s); solid funding stream for next overlapping upgrade increment(s)

- making schedule the priority for releasing available capability and not requiring (or expecting) a “yes” vote from every functional organization prior to decision milestones
- making sure that users are trained and prepared to receive the new capability

Model Characteristics

The proposed acquisition process is divided into four phases (Figure 20). Each phase begins with either a milestone decision authority-level decision review or a milestone event to ensure adequate knowledge is available to proceed to the following phase, which is associated with increasing levels of investment.

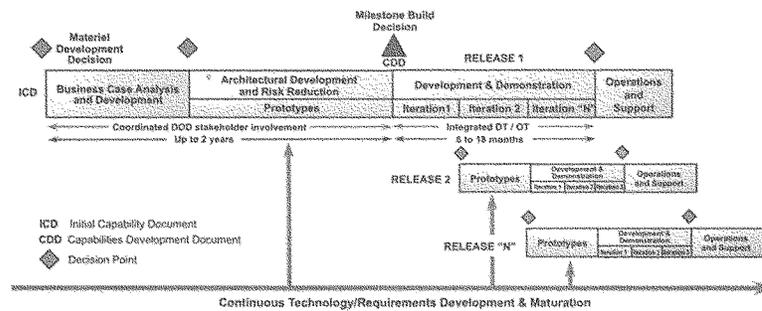


Figure 20. A New Acquisition Process for Information Technology

The new model characteristics, a number of which are consistent with DOD’s new acquisition process model, are critical to success:

- **Sound structure and effective oversight.** The model is divided into four phases:
 1. **Business Case Analysis and Development.** Establish the need for the proposed capability and develop the concept for the proposed solution. The phase begins once an Initial Capability Document and draft Concept of Operations are approved, based on an identified mission need.

2. **Architectural Development and Risk Reduction.** The core architecture is built and architecturally significant features demonstrated. Prototyping begins during this phase and continues throughout the acquisition life cycle to assess the viability of technologies and minimize high-risk features, while simultaneously refining user capability expectations.
 3. **Development and Demonstration.** The period when operational capability is built and delivered for a discrete number of releases. Capabilities are prioritized and parsed into groupings to establish release baselines for the sub-programs. Includes development of training programs and testing in realistic environments to ensure successful fielding of new capabilities.
 4. **Operations and Support.** Provides materiel readiness, user training, and operational support over the total program life cycle.
- **Enhanced stakeholder engagement and analytical rigor at the enterprise level.** Today's practice of not extending the architecture and engineering systems analysis rigor from the enterprise level down to the program level has resulted in poor acquisition outcomes. While the proposed acquisition may well serve the individual DOD component, it is often ill equipped to foster modern "enterprise" behavior. Under the proposed process, program initiation depends on a credible business case based on analytical rigor applied and reviewed at the program and enterprise levels. The business case should demonstrate that while the solution may serve the unique needs of the individual DOD component, it must also add value when appropriate to the larger enterprise. There is a natural tension between the goals of the individual program and the goals of the enterprise. Individual programs often can quickly develop capabilities if they ignore enterprise needs. However, these capabilities are not likely to be interoperable. Activities that do not seem to need interoperability mechanisms today often will tomorrow. Further, as one looks across the enterprise at a set of mission-specific program developments, one inevitably sees redundancy and inefficiency.

Nonetheless, processes for managing the trade-offs between local program-based decision making and enterprise coordination are themselves time-consuming. The model proposed here puts specific emphasis on this problem by calling for up-front analysis (when requirements are most flexible and costs are lowest) so that good decisions—including decisions about enterprise integration—are made

when they can have high impact. Assurance of this enterprise compliance is a critical role of the DOD CIO.

- **Acquisition processes and governance** must ensure full and effective integration of CIO roles and responsibilities for IT professionals—throughout the process.
- **Prototyping.** Each increment of development must be supported by early and continuous prototyping to ensure that the necessary technologies and functionality will be available in real time to support development. The model embraces continual technology development, prototyping, and the accompanying requirements maturation throughout the acquisition life cycle.
- **Training and testing.** To successfully field capabilities, comprehensive testing, training, and follow up user support is required. The extensive prototyping should enable user feedback and training program development to be effectively incorporated into the program early and continue throughout development.

The model also introduces some important new characteristics:

- **Multiple rapidly executed increments/releases of capability.** Each increment would be responsive to a single approved Capability Development Document (CDD) and each would be fully funded. In an important departure from current practice, each increment of capability would include multiple (“N”) capability releases, each a useful stand-alone capability consistent with the approved CDD. The need for more than “N” releases would trigger a new CDD and subsequently a new increment. Each release would be developed in approximately 18 months or less. Releases, in turn, are sub-divided into multiple iterations to facilitate assessment of progress by prioritizing work scope into a smaller subset of functionality that is tested and potentially deployable. It is important to emphasize that smaller increments allow for better synchronization with enterprise capabilities now evolving at the same rapid rate as the program capabilities. More frequent releases allow opportunities to continually address integration and interoperability issues rather than having to get them all “right” in the requirements phase.

All releases would be accommodated by the baseline for the increment or, consistent with recent changes to statute, could be treated as sub-programs with unique cost, schedule, and performance parameters.

Prototyping will typically be employed in each release, but whether it is necessary will depend on the capability goals of the particular release. Deployment would be based on the results of testing and approved by the acquisition decision authority. In short, this approach replaces the current “big bang” model with a responsive alternative that provides incremental mission capability much sooner.

- **Thoughtful satisfaction of requirements.** The objective of this new model is to develop and deploy the highest priority mission capability first. Therefore, capabilities defined in the CDD should be prioritized, and, where appropriate, grouped into a limited number of time-phased releases that correspond to mission priority. While each increment will be supported by an approved CDD, an agile approach would, with the active engagement of the requirements community, allow for (and encourage) reprioritization of requirements for each iteration and release (and for the increment as a whole) based on subsets of functionality to prevent delay and facilitate rapid development/deployment. While rapid introduction of smaller releases of capability is attractive, it must be moderated by potential confusion in the field and the training required in support of each release. Therefore, tight coordination between user operators and developers is required to schedule each release.
- **Better informed cost estimates.** By decomposing and managing an acquisition in well understood and thoughtfully described smaller units, the Department’s process for creating realistic initial cost and schedule baselines has the potential for significant improvement. As noted by the earlier references to RAND, GAO, and Defense Science Board reports, the acquisition and resourcing processes do not always produce realistic cost and schedule estimates; hence program buy-in with very optimistic estimates is common while resulting cost and schedule performance is poor. To enhance the fidelity of cost and schedule estimates, the new model departs from the current practice of requiring a cost estimate only at program initiation. Instead, each release is treated as a sub-program for purposes of cost and schedule estimating and reporting. Following the initial cost estimate at the “build decision” (program initiation), estimates are refined after each release to reflect program results based upon realized performance and forward-looking priorities. The Department should also embark upon an effort to improve analytical rigor by expanding the analysis beyond previous DOD cost information; estimates should leverage all relevant cost databases. The task force

recognizes that experienced analysts necessary to achieve this fidelity are not currently available in the Department or the Services.

- **Contracting and funding.** We envision a lean, commercially based acquisition model that emphasizes extensive analysis prior to development, a flexible requirements process, better cost estimates, and modular and incremental development and fielding over shorter cycles. This model implies that each development increment will result in less than the ultimate capability—a change that the Department and Services should be prepared to accept. In addition, and important to the success of this new model, the contract vehicles used to acquire these increments must be flexible enough to allow for changes in delivered capability within a particular increment or allow capabilities to be deferred to subsequent increments if the capability realization must be delayed without onerous cost consequences to the government.

This contracting approach will require careful definition of the expected increments of capability as well as flexibility within the contracting vehicle to allow the program manager to defer based on his or her own authority. When the requirements for subsequent increments of capability are not sufficiently refined to support detailed cost estimating, DOD should embrace the concept of “level-of-effort” funding. This approach will ensure that adequate funding is continuously available to support multi-increment developments and, as important, to upgrade and sustain fielded capability. It will also require significant training and culture change for DOD contracting officers and program officials. This model, in effect, “fixes” budget and program timelines. The burden, then, is on the program to define capabilities that can be fit into those constraints. Finally, just as there is no substitute for acquisition leadership experience, the same is true for contractors. For contract award, program managers need to strongly consider relevant contractor experience and past performance, especially in large acquisitions, and ensure that key personnel are committed for the duration of the project.

- **More frequent but less formal progress reviews.** As defined earlier, progress in today’s acquisition oversight process is accomplished through overlapping and protracted coordination, which tends to make change at the margin rather than enable substantial trade-offs. Instead, the IT acquisition process requires continuous “hands-on” oversight beginning at the Material Development Decision via quarterly program reviews to get first-hand progress as reported by the program manager. Program

reviews, tied when possible to release “iterations,” will expose flawed programs or poor design early while the program is small and, by forcing early integration, it avoids the downstream issues resulting in more robust and maintainable designs. Multiple decision points can be interspersed throughout the program based upon the inherent risk and program life cycle.

- **Tailored testing practice.** Test planning, test execution, and post-deployment support cannot be based upon traditional thinking that scope and content is fixed at the beginning. Instead of a single test event, acquisition activities rely on development test events after each iteration and operational testing to support decisions to field the release. An especially important planning consideration is the use of automated testing to allow effective iterative testing of previous functionality.
- **Modular, open-systems approach.** In an operational setting, the IT acquisition process requires movement to an open architecture structured for ease of upgrades. A fundamental step is to partition the design into a hierarchy of individual modules (both hardware and software) with well defined interfaces based on open standards, such that the inputs and outputs of a module are effectively isolated from the specific design utilized inside that module. Thus, so long as interface requirements are satisfied, changes can be made within a module without impacting higher level system functionality and reuse of modules is enabled.

The use of standards-based reference models, well-defined and published interfaces, and test and acceptance criteria ensures transparency and the widest range of options in vendor selection. A standards-based, open system serves to mitigate the specification of a system for a vendor’s proprietary product, but also helps to prevent restrictive intellectual property rights issues and vendor lock-in. This practice clearly follows commercial best practices; however, in rare instances a more deliberate government specific policy may be needed to increase the information assurance position of critical systems.

The growing importance of information demands focused management of the information technology enterprise. The policy revisions proposed here are consistent with current best commercial practice, have been employed successfully by industry (and to a far lesser degree in DOD), and reflect principles that are both effective and applicable to the DOD IT acquisition environment. The employment of an agile approach will increase IT capability,

program predictability, reduce cost, and decrease cycle time—all business imperatives, especially in a potentially austere budget environment.

Model Phases

Each phase of the new acquisition process for information technology is described in more detail below.

Business Case Analysis and Development

The Business Case Analysis and Development phase establishes the need for the proposed capability and develops the concept for the proposed solution. During this phase designers will develop an understanding of the operational objectives, the operator's perspective of the criteria for success, and the implications for architectural imperatives and complexity issues. This activity includes understanding the goals, rules, data flows and interdependencies of the proposed system with existing systems in the mission context. It also includes cost/benefit trade-off analysis (the analysis of alternatives and business case analysis) to not only identify the preferred solution but also to quantify benefits of the proposed solution. The sponsoring component can accomplish this via business/system context diagrams, modeling, and data transaction diagrams to illustrate key attributes in context of the larger enterprise.

The phase begins with a Materiel Development Decision review led by the milestone decision authority. The purpose of the review is to gain approval for the Initial Capability Document and draft Concept of Operations resulting from the analysis of current mission performance and potential concepts across the DOD components, international systems from allies, and cooperative opportunities. Guidance for the analysis to be conducted during the phase is also approved. Approval of these documents is required for entrance into the phase.

The DOD component(s) accomplish cost/benefit analysis by balancing incremental investments with returned value (qualitative and quantitative results) that can offer accountability with stakeholders by tracking results over time. Analyses consider the probability and confidence levels of performance, scalability, cost growth, changes in commercial performance and standards, enterprise benefits, and range of uncertainty.

The Business Case Analysis and Development Phase exit criteria are met when the business case has been completed, materiel solution options for the

capability need identified, and the approved Initial Capability Document recommended.

Architecture Development and Risk Reduction

The purpose of the Architecture Development and Risk Reduction phase is to build the core architecture, demonstrate the architecturally significant features, and gain user support for the proposed conceptual technical solution. While the concept of prototyping begins during this phase, continuous prototyping activity is needed throughout the acquisition life cycle to assess the viability of technologies and minimize high-risk features while simultaneously refining user requirements. Therefore, it is expected that technology development and prototyping activity continues in support of follow-on releases and/or increments of capability. Completion of this phase of activity does not mean that a program has been initiated.

Entrance into this phase depends upon an approved business case including a proposed materiel solution(s), economic analysis, draft CDD, full funding for architecture development and risk reduction activities, and enterprise engineering artifacts highlighted in the earlier phase.

Activities in this phase begin with a decision review marking the formal entry point into architecture development and risk reduction. At this review, the milestone decision authority assures that the exit criteria of the Business Case Analysis and Development phase have been met and approves the proposed materiel solution and the technology development strategy, which describes the phase activities, funding, and objectives.

A System Requirements Document is developed based on capabilities outlined in the draft CDD. These prioritized requirements are subsequently time-boxed and decomposed into lower level requirements. A time-phased workload assessment is needed to identify the manpower and functional competency requirements for successful program execution and the associated staffing plan, including the roles of government and non-government personnel.

A list of known or probable Critical Program Information and potential countermeasures in the preferred system concept is also initiated during this phase. This activity is extended throughout the acquisition life-cycle to identify critical technologies and prototypes that may inform program protection and integration in subsequent acquisition activities.

Multiple risk reduction demonstrations focused on small subsets of functionality may be necessary before the user and developer agree that a proposed technology solution is affordable, militarily useful, enterprise aligned, and based on mature, demonstrated technology. (Enterprise alignment refers to synchronization and prioritization in terms of contribution of the larger environment.) Leveraging draft operational requirements, the program manager defines the system architecture, system-of-systems functionality and interfaces, and complete hardware and software detailed design for the system and increment.

The DOD component's CIO conducts IT maturity assessments against standards set by the American National Standards Institute, Institute of Electronic and Electrical Engineers, or The Open Group's Architectural Framework to assess the proposed solution and its ability to support an open architecture framework while addressing information security concerns. While the objective is to develop IT systems based on mature technologies, in rare instances where this may not be the case, the milestone decision authority, in consultation with the DOD CIO, determines whether TRAs and TRLs are necessary for acquisitions involved in fundamental advances in science and engineering underlying the cyber infrastructure and leap-ahead technologies (i.e., acquisitions truly involved in technology-push).

The Technology Development Strategy includes a description of how the materiel solution is divided into increments, releases, and capability iterations. It also includes strategies needed to rapidly incorporate technology solutions and establish the number of prototype units or engineering development models that may be produced in support of development and demonstration activities. The initial capability increment, including the sub-division of capability into releases, is to be defined by the Capability Development Document. Each release should not exceed approximately 18 months and should be further sub-divided into iterations (nominally three in number). Each iteration represents a subset of useful functionality that is tested and potentially deployable. Because of operational considerations, iterations are typically bundled together, operationally tested, and deployed via a release.

During Architecture Development and Risk Reduction, the user prepares the Capability Development Document to support the acquisition program. The CDD builds on the Initial Capability Document and provides the detailed operational performance parameters necessary to complete the proposed system design. These requirements are prioritized and parsed into groupings to establish

baselines for initial and subsequent releases. The program manager decomposes these operational requirements by translating the requirements into features of functionality. These features are further decomposed and prioritized into smaller units of functionality and incorporated into the Technology Development Strategy planning.

The project exits Architecture Development and Risk Reduction when an affordable program increment of militarily useful capability has been identified and approved by the proposed user; the technology approach for that program has been assessed; architectural and design risks have been identified and assessed; cost estimates are complete; and a system or increment can be developed within a short timeframe to achieve the time-certain mandates imposed by Congress.

Development and Demonstration

The purpose of the Development and Demonstration phase is to build and deliver operational capability for a discrete number of releases. Releases beyond that planned number restart the entire process and would typically be associated with a follow-on increment.

Entrance into this phase depends upon an approved CDD and proposed acquisition strategy and acquisition program baseline for “N” releases established at the Milestone Build Decision. As noted earlier, the requirements are prioritized and parsed into groupings to establish release baselines for the sub-programs. Likewise, appropriate planning documentation similar to those required for the current Milestone B decision is approved by the DOD component. In contrast to today’s acquisition paradigm, these documents are considered “living documents” requiring updates at the end of a release. Finally, the program is fully funded; therefore, all releases for a given capability increment are fully funded at the Milestone Build Decision.

The Development and Demonstration Phase activities begin with a milestone decision review marking the successful completion of architecture development and risk reduction and commitment to develop and operationally field mission capability. At the Milestone Build Decision, the milestone decision authority approves the acquisition strategy and the acquisition program baseline, which is documented in a decision memorandum.

Leveraging the requirement priority set forth in the validation process, the program manager updates the architecture as necessary and completes design of the initial release with increasing level of detailed design associated with the first iteration. This includes system and system-of-systems functionality and interfaces, and complete hardware and software detailed design for the release. Also, the development of user training and implementation plans coordinated with the proposed releases are completed and verified through testing.

Following design activity, the development effort is focused at the iteration-level to produce system capability needed to satisfy approved requirements. Developmental test and evaluation is conducted to assess technical progress against critical technical parameters and, where appropriate, the use of modeling and simulation to demonstrate system and system-of-systems integration.

Following the nominal completion of three iterations, an Initial Operational Test and Evaluation (IOT&E) is accomplished prior to operationally fielding a release. An operational release is preceded by a decision from the milestone decision authority approving each release and follows successful IOT&E. IOT&E and fielding decisions are conducted for each release until the program satisfies the requirements for the increment.

Operations and Support

The Operations and Support phase provides materiel readiness and operational and user support over the total program life cycle. Training users in the new capability and providing support for initial use is critical to successfully fielding the capability. Training programs should be tested and evaluated to assure that they are comprehensive and effective. Life cycle sustainment planning and execution seamlessly span a system's entire life cycle. It translates force provider capability and performance requirements into tailored product support to achieve specified and evolving life cycle product support availability, reliability, and affordability parameters. Entrance into this phase depends on meeting the following criteria: an approved Life Cycle Support Plan and a successful Deployment Production Decision.

Subsequent Increments

Consistent with an evolutionary approach, multiple increments may be required to satisfy the capability need. In that case, each follow-on increment typically begins at the Milestone Development Decision and capitalizes on

continuous technology development and prototyping activity. Additional increments start the decision process again and must have approved requirements, be based upon mature technologies, have an acquisition strategy and baseline approved by the milestone decision authority, and be fully funded.

Deciding When to Use the New IT Acquisition Process

It is important to clarify when to use the new IT acquisition process versus the improved DOD 5000.02 process for major weapon systems and communication satellites. In addition, it is also necessary to reduce potential confusion about technology development.

The use of the improved DOD 5000.02 process for major weapon systems is required when there are many design trade-offs for both hardware and IT systems and for partitioning the functions and interoperability of embedded IT systems and subsystems in a new system, while assuring interoperability and network compatibility with the larger enterprise. At the same time there are likely to be areas of needed technology development that require advances in science and engineering that have little or nothing to do with IT—such as new material properties, increased speed, or stealth. This later scientific and engineering technology development should not be confused with the traditional jargon of the IT community that defines technology development nearly interchangeably with software development and hardware integration.

The use of the new IT acquisition process is for new or replacement stand alone IT systems and subsystems or for replacement IT systems embedded in existing weapon systems that are to be upgraded when there is little or no change in the hardware not associated with IT. It may also be appropriate to use the IT acquisition system process concept within the 5000.02 process for new embedded IT systems in a major weapon system acquisition as the IT technology could otherwise be a few generations old at IOC.

While one could argue that this required new decision could add confusion to the process, one could also argue that if the leadership and program managers cannot sort out this high-level decision they have no chance of effectively managing or overseeing the program.

Chapter 7. Summary and Recommendations

As stated at the outset of this report, IT acquisitions continue to grow in size, cost, and complexity, and the percentage of embedded IT in weapon systems is growing. Yet at the same time many IT acquisition programs have not met expectations and attempts to streamline the acquisition progress have not met with success. Cycle times continue to lengthen and costs increase. In the view of the task force, there are two chief causes for these circumstances: (1) there is not sufficient leadership with proven experience to structure executable programs and (2) the DOD IT acquisition process is inconsistent with the rapid pace of commercial IT technology cycles. DOD must take action to remedy these problems. Toward this end, this chapter summarizes the key findings and recommendations of the task force.

Statutory Restrictions

The task force believes that the statutory framework is workable and is not a major impediment to improving IT acquisition within DOD. Therefore, no recommendations are offered in this area. The main issue with regard to statutory influence is that Congress has lost confidence in DOD's execution of IT programs, which has resulted in increasing program scrutiny and budget actions (generally funding cuts) for programs that are faltering. Since DOD implementation of IT acquisition has fallen short, Congress has added additional constraints on reporting and management, these could become problematic when and if DOD begins executing programs well.

Acquisition Policies

Acquisition policies (DOD Directive 5000.1 and Instruction 5000.2) are principally designed for programs where technology development for hardware and software is a critical component. The recent release of DOD Instruction 5000.02, implemented December 2008, offers improvements to the process but do not address the fundamental challenges of acquiring information technology for its range of uses in DOD. Instead, a new acquisition approach is needed that is consistent with rapid IT development cycles and software-dominated acquisitions.

RECOMMENDATION 1. NEW ACQUISITION PROCESS FOR INFORMATION TECHNOLOGY**The Secretary of Defense should:**

- Recognize that the current acquisition process for information technology is ineffective. Delays and cost growth for acquisition of both major weapons systems and information management systems create an unacceptable risk to national security.
- Direct the USD (AT&L) and the Vice Chairman, Joint Chiefs of Staff to develop new acquisition and requirements (capabilities) development processes for information technology systems. These processes should be applicable to business systems, information infrastructure, command and control, ISR systems, embedded IT in weapon systems, and IT upgrades to fielded systems.
- Direct that **all** personnel within the Office of the Secretary of Defense, the Joint Staff, and the Services and agencies involved with acquisition be accountable to ensure that their efforts are focused on the improvement, streamlining, and success of the new process.

The USD (AT&L) should lead an effort, in conjunction with the Vice Chairman, Joint Chiefs of Staff, to develop new, streamlined agile capability (requirements) development and acquisition processes and associated policies for information technology programs.

The task force proposes a new process, modeled on successful commercial practices, for the rapid acquisition and continuous upgrade and improvement of IT capabilities. The process is agile, geared to delivering meaningful increments of capability in approximately 18 months or less, and leverages the advantages of modern IT practices. Multiple, rapidly executed releases of capability allow requirements to be prioritized based on need and technical readiness, allow early operational release of capability, and offer the ability to adapt and accommodate changes driven by field experience.

The process requires active engagement of the user (requirements) community throughout the acquisition process, with “capability needs” (vice requirements) constructed in an enterprise-wide context. It is envisioned that

requirements will evolve to “desired capabilities” that can be traded off against cost and IOC to get the best capability to the field in a timely manner. Systems analysis should be used to determine capability needs trade-offs rather than the typical functionality, cost, and IOC dates. A modular, open-systems methodology is required, with heavy emphasis on “design for change,” in order to rapidly adapt to changing circumstances. Importantly, the process needs to be supported by highly capable, standing infrastructure comprising robust systems engineering, model-driven capability definition, and implementation assessments—to reduce risk, speed progress, and increase the overall likelihood of repeated successes. Early, successive prototyping is needed to support the evolutionary approach. In addition, key stakeholders—the CIO, PA&E, DDR&E, OT&E, Comptroller, operational users, and others—need to be involved early and constructively in the process, prior to the milestone build decision.

Testing methodologies and procedures need to be engaged early and often in the acquisition process, with integrated and continuous development and operational testing practiced during the development and demonstration phase for each capability release. Contracting vehicles need to be devised that are flexible enough to support this agile process—that will allow for changes in delivered capability within a particular increment, as well as allow capability to be deferred to subsequent increments if needed. Crucial to the success of this new process is continuity of funding, to maintain a solid funding stream for following, sometimes overlapping, capability releases. Along with the flexibility built into the process, relevant metrics need to be developed to continuously track IT acquisitions to ensure that the expected capability is being provided, costs are being managed, and the schedule to initial capability is on track. Finally, just as there is no substitute for acquisition leadership experience, the same is true for contactors. For contact award, program managers need to strongly consider relevant contactor experience and past performance especially in large acquisitions and ensure that key personnel are committed for the duration of the project.

Implementation training for users is integral to the process. Training packages need to be designed and tested before each release. After fielding, testing of system effectiveness and the supporting training needs to be performed to provide feed-back to system developers.

The task force believes that this new process will have applicability over a broad range of new DOD IT acquisitions and upgrades to existing national

security systems (including command and control systems), IT infrastructure, and other information systems (Figure 21). IT is not simply a niche consideration—it touches a wide range of systems and, in turn, enables a wide range of capabilities.

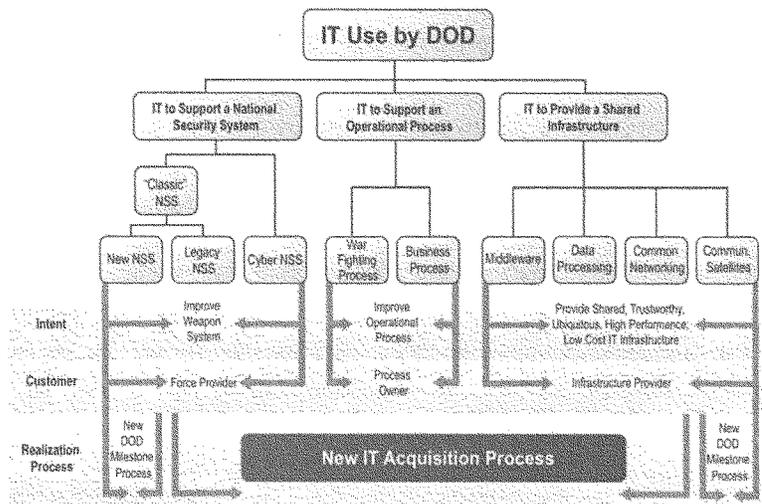


Figure 21. An Information Technology Acquisition Framework

Roles and Responsibilities of the ASD (NII)/DOD CIO

The DOD CIO function is currently housed in the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII)/DOD CIO). DOD CIO responsibilities are delineated within titles 10, 40, and 44 of the U.S. Code. As designated in legislation, the ASD (NII)/DOD CIO reports directly to the Secretary of Defense—a reporting chain that the task force believes is critical and must continue in order for the ASD (NII)/DOD CIO to have the necessary authority to carry out important department-wide functions.

The ASD (NII)/DOD CIO should have strong authorities and responsibility for information policy vision, architecture, infrastructure, metadata and other standards, spectrum, information assurance, interoperability, and enterprise-wide systems engineering. The ASD (NII)/DOD CIO should be the Department's single authority for certifying that IT acquisitions comply with an enterprise-wide

architecture and should continually review ongoing programs for architectural compliance. He or she should also be a ruthless designer of “the enterprise” infrastructure and should approve IT program manager training and certification programs. However, the task force believes that some of the functions delineated here need to be strengthened in order to ensure that the full responsibilities of the office can be effectively executed.

These functions are also applicable to CIOs at the Service and agency level. To execute the above responsibilities, Service and agency CIOs should also directly report to the head of the Service or agency, as required by legislation.

RECOMMENDATION 2. ASD (NII)/DOD CIO RESPONSIBILITIES

The ASD (NII)/DOD CIO should actively exercise his or her authority to certify that all IT acquisitions are consistent with the Department’s net-centric architecture.

The ASD (NII)/DOD CIO must have strong authorities and responsibilities for enterprise-wide information policy vision, architecture, infrastructure, metadata and other standards, spectrum, interoperability, information assurance, and system engineering.

Certain capabilities in the OASD (NII)/DOD CIO must be strengthened in order to more effectively execute these responsibilities—in particular, system engineering, information assurance, and network integration.

In the Services and agencies, the CIOs should also have strong authorities and responsibilities for system certification, compliance, applications development, and innovation.

All CIOs should approve IT acquisition program manager training and certification and advise the personnel selection process.

The DOD CIO, supported by CIOs at the Services and agencies, should be responsible for certifying that systems and capabilities added to the enterprise do not introduce avoidable vulnerabilities that can be exploited by adversaries.

System vulnerability to sophisticated adversary threats, and information and mission assurance should be addressed throughout program development, particularly in the early stages during the business case analysis and development phase. As new capabilities, infrastructure, and applications are added to a system, this same assessment should be continuously monitored with particular emphasis on source code analysis and supply chain risk assessment. A robust testing program must also be established to minimize the introduction of new vulnerabilities. New capabilities need to be tested in realistic test beds under a variety of threat scenarios.

While not the centerpiece of this report, the task force believes that information and mission assurance must be an integral element of the IT acquisition process, not an afterthought. IT is far too important to the Department's war fighting and business endeavors to neglect information and mission assurance, as the consequences of doing so can not only undermine the current system but also other connected capabilities as well. In this context, it is instructive to remember that there is no way to test a large IT system to assure that you "got what you wanted" and only what you wanted. Thus, since it is not possible to assure that an IT system is entirely safe and reliable, operators (combatant commanders) must develop field-testing procedures; tactics, techniques, and procedures; and concepts of operations to operate with degraded systems.

Milestone Decision Authority Roles and Responsibility

Clear roles and responsibilities of those with milestone decision authority are essential if a new acquisition process is to be successful and the desired outcomes achieved. The lack of clarity in this regard is one of the most significant impediments to successful implementation of the current process. The task force believes that the preferred approach should be delegation to the lowest level milestone decision authority consistent with program risk.

Furthermore, acquisition authority and expertise within OSD is currently spread across several organizations—under the USD (AT&L), the ASD (NII), and in the Business Transformation Agency—resulting in diffusion of capability and a competition among scarce resources. At the Service level, similar disaggregation of responsibility also exists. This disaggregated approach seems inefficient to the task force, resulting in a lack of enterprise-wide architecture and coordination. Qualified IT acquisition and systems analysis and architecture personnel are scarce and should not be spread among separate OSD

organizations. Given the speed with which information technology advances, this disaggregation exacerbates the ability to maintain currency and coordination within the acquisition workforce.

It is important to recognize that IT acquisition requirements are different and, because IT touches nearly everything acquired by the Defense Acquisition Executive (USD (AT&L)), it is more than a side consideration. Bringing together the expertise from many organizations into a single one will help to ensure that the unique attributes of IT acquisition programs is better understood. In addition to the matter of milestone decision authority responsibilities and organization, the Defense Acquisition Executive advisory staff (DDR&E, PA&E, OT&E, Comptroller, and others) issue definition and resolution process often contributes to extended IT acquisition times.

RECOMMENDATION 3. ACQUISITION AUTHORITIES AND ORGANIZATION

The USD (AT&L) is responsible for all acquisitions, the acquisition workforce, and is the milestone decision authority for all MDAP, MAIS, and special interest programs. The USD (AT&L) should:

- aggressively delegate milestone decision authority commensurate with program risk
- implement a more effective management and oversight mechanism to ensure joint program stability and improved program outcomes

Consolidate all acquisition oversight of information technology under the USD (AT&L) by moving into that organization, those elements of the OASD (NII)/DOD CIO and Business Transformation Agency responsible for IT acquisition oversight. The remainder of OASD (NII)/DOD CIO is retained as it exists today, but should be strengthened as indicated in the previous recommendation.²⁹

29. We note that there was not a consensus view within the task force concerning this recommendation; a dissenting view is included in Appendix A.

Acquisition Expertise

A high degree of relevant technical and proven management capability is needed for IT system acquisition leadership. In addition, a set of IT domain experts are needed within the acquisition community to support acquisition oversight and decision-making. OSD and the Services need IT acquisition staff with extensive experience in large-scale, embedded, and commercial IT.

Today, the subject matter competencies required for successful enterprise IT system acquisition are too often missing in government managers responsible for program execution. Skills in program administration are confused with skills in operational process design and/or with skills in IT. Contracting, budgetary, and organizational design debates crowd out concepts of operations and system engineering debates. Further, architecture is too often viewed as a paper exercise rather than a model-driven, analytically supported, and rigorous engineering process, incorporating enterprise-wide considerations for functionality and interface definition. Within the Department, IT expertise is scarce and the competition for talent is increasing.

There is no substitute for experienced program managers with track records of proven success. In a review of major IT acquisition programs where cost, schedule, or quality and performance were issues, three root causes emerged. First, senior leaders lacked experience and understanding. Second, the program executive officers and program managers had inadequate experience. Third, the acquisition process was bureaucratic and cumbersome, where many who are not accountable must say “yes” before authority to proceed is granted. Some of these issues have been discussed previously in this report, but among these problems, lack of experience dominated. The Department has mechanisms to acquire experienced talent including the Intergovernmental Personnel Act and other special hiring authorities. In general the DSB has found that these programs are underutilized.

The experience and qualifications of OSD and Service leaders, and program executive officers and program managers is critical to making the *right judgments* to begin a program with executable objectives and then manage it to successful completion.

RECOMMENDATION 4. ACQUISITION EXPERTISE

The Secretary of Defense shall require that the Defense Acquisition Executive (USD (AT&L)) and the component acquisition executives have proven and relevant business experience in the appropriate areas of acquisition, product development, and management. Such qualifications apply to the ASD (NII)/DOD CIO and Service and agency CIOs as well.

The USD (AT&L) must work with Service and agency acquisition executives to improve the capabilities and selection process for program executive officers and program managers.

The USD (AT&L) shall direct the Defense Acquisition University, in coordination with the Information Resources Management College, to integrate the new acquisition model into their curriculum.

Conclusion

The task force believes that actions in these four areas will improve the acquisition of information technology in DOD: (1) acquisition policies and process, (2) roles and responsibilities of the CIO, (3) milestone decision authority roles and responsibilities, and (4) acquisition leadership expertise. But caution is offered that emphasis and focus only on the acquisition process is not enough. While the task force feels that a new process is needed that better takes into consideration the unique aspects of information technology, it alone will not yield success. If the matters associated with responsibilities and authorities, organization, and expertise are not also addressed, the new process proposed here is likely to meet with the same outcomes as process improvements recommended by other groups who have studied this issue. This set of recommendations is designed to both streamline the IT acquisition process and address the fundamental problems that exist in the system today.

Appendix A. Dissent to Report

I am gratified to see the changes to the original report which remove the recommendation to move NII under AT&L. However, having removed that recommendation, the report is not particularly consistent in other recommendations. Since NII will remain as a direct report to the Secretary of Defense, the lack of any discussion of using the Clinger-Cohen procedures to acquire IT systems is disturbing. I disagree that the DOD would be better served by not allowing the use of the alternative acquisition procedures available through Clinger-Cohen. The DOD could acquire IT systems in the context of Process Improvement where a business case is developed which combines Process Changes with IT acquisition. This would be particularly useful for the Business Transformation Agency programs. Today, Clinger-Cohen allows the Secretary of Defense to declare any IT program as a National Security System and leave only Clinger-Cohen requirements for meeting standards from that acquisition, so anything the report contemplates as an improvement by eliminating the Clinger-Cohen acquisition process can be done today, but the department will lose an alternative process to use when it is advantageous.

With only IT acquisition oversight of IT programs moving from NII to AT&L, the number of NII personnel who would transfer would be less than six. NII would have to have people reviewing the related programs in order to form advice on possible changes which would lead to a better integrated result. Budget reviews would still be required, Congressional interface would still be required, and there would be increased overlap in those functions between AT&L and the CIO. If so few people would move, then why move anybody? Such a recommendation is inconsistent with the dialog in the report suggesting that concentration of the few IT professionals in OSD is desirable. Perhaps a better recommendation would be for AT&L to reorganize within its resources to have a focal point for IT as it applies to embedded systems and those IT systems which are determined to be National Security Systems. That office could be the major coordination vehicle with NII to maximize the utility of the Clinger-Cohen process to areas where it might be more effective than use of the 5000 processes.

John Stenbit

Terms of Reference and Legislative Directive



ACQUISITION,
TECHNOLOGY
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

MAY 01 2008

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board Task Force on the
Department of Defense Policies and Procedures for the Acquisition of
Information Technology

In accordance with section 887 of the National Defense Authorization Act for
FY 2008 (PL 106-65), you are requested to carry out a review of Department of Defense
policies and procedures for the acquisition of information technology.

The purpose of the Task Force will be to determine whether existing acquisition
policies and processes provide the foundation necessary for an effective acquisition
model and to identify recommended improvements to enhance the Department's
approach to information technology acquisition.

The matters addressed by the review shall include the following:

- (1) Department of Defense policies and procedures for acquiring information
technology, to include national security systems, major automated information
systems and business information systems, and other information technology.
- (2) The roles and responsibilities in implementing such policies and procedures of:
 - (a) The Under Secretary of Defense for Acquisition, Technology, and
Logistics;
 - (b) Chief Information Officer of the Department of Defense;
 - (c) The Director of the Business Transformation Agency;
 - (d) The Service Acquisition Executives;
 - (e) The Chief Information Officers of the Military Departments;
 - (f) Defense Agency acquisition officials;
 - (g) The Information Officers of the Defense Agencies, and;
 - (h) The Director of Operational Test and Evaluation and the heads of the
operational test organizations of the military departments and the
Defense Agencies.
- (3) The application of such policies and procedures to information technologies
that are an integral part of critical weapons or weapons systems.



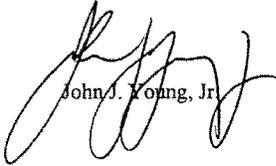
- (4) The requirements of subtitle III of title 40, United States Code, and chapter 35 of title 44, United States Code, regarding performance-based and results-based management, capital planning, and investment control in the acquisition of information technology.
- (5) Department of Defense policies and procedures for maximizing the usage of commercial information technology while ensuring the security of the microelectronics, software, and networks of the Department.
- (6) The suitability of Department of Defense acquisition regulations, including Department of Defense Directive 5000.1, Department of Defense Instruction 5000.2, and the accompanying milestones, to the acquisition of information technology systems.
- (7) The adequacy and transparency of metrics used by the Department of Defense for the acquisition of information technology systems.
- (8) The effectiveness of existing statutory and regulatory reporting requirements for the acquisition of information technology systems.
- (9) The adequacy of operational and development test resources (including infrastructure and personnel), policies, and procedures to ensure appropriate testing of information technology systems both during development and before operational use.
- (10) The appropriate policies and procedures for technology assessment, development, and operational testing for purposes of the adoption of commercial technologies into information technology systems.

A report will be submitted to the Secretary of Defense and Congress not later than January 28, 2009.

Where relevant, the Task Force should draw upon previous DSB reports to include the 2006 Summer Study on Information Management for Net Centric Operations, the Task Force reports of Mission Impact of Foreign Influence on DoD Software, and High Performance Microchip Supply.

The study will be sponsored by me as the USD(AT&L) and the ASD(NII). Dr. Ron Kerber and Mr. Vince Vitto will serve as the Task Force Chairpersons. Mr. Skip Hawthorne, OUSD(AT&L) will serve as the co- Executive Secretary and LTC Karen Walters, USA, will serve as the DSB representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.



John J. Young, Jr.

110TH CONGRESS }
1st Session

HOUSE OF REPRESENTATIVES

{ REPORT
110-477

NATIONAL DEFENSE AUTHORIZATION ACT
FOR FISCAL YEAR 2008

CONFERENCE REPORT

TO ACCOMPANY

H.R. 1585



DECEMBER 6, 2007.—Ordered to be printed

SEC. 887. DEFENSE SCIENCE BOARD REVIEW OF DEPARTMENT OF DEFENSE POLICIES AND PROCEDURES FOR THE ACQUISITION OF INFORMATION TECHNOLOGY.

(a) **REVIEW REQUIRED.**—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall direct the Defense Science Board to carry out a review of Department of Defense policies and procedures for the acquisition of information technology.

(b) **MATTERS TO BE ADDRESSED.**—The matters addressed by the review required by subsection (a) shall include the following:

(1) Department of Defense policies and procedures for acquiring national security systems, business information systems, and other information technology.

(2) The roles and responsibilities in implementing such policies and procedures of—

(A) the Under Secretary of Defense for Acquisition, Technology, and Logistics;

(B) the Chief Information Officer of the Department of Defense;

(C) the Director of the Business Transformation Agency;

(D) the service acquisition executives;

(E) the chief information officers of the military departments;

(F) Defense Agency acquisition officials;

(G) the information officers of the Defense Agencies; and

(H) the Director of Operational Test and Evaluation and the heads of the operational test organizations of the military departments and the Defense Agencies.

(3) The application of such policies and procedures to information technologies that are an integral part of weapons or weapon systems.

(4) The requirements of subtitle III of title 40, United States Code, and chapter 35 of title 44, United States Code, regarding performance-based and results-based management, capital planning, and investment control in the acquisition of information technology.

(5) Department of Defense policies and procedures for maximizing the usage of commercial information technology while ensuring the security of the microelectronics, software, and networks of the Department.

(6) The suitability of Department of Defense acquisition regulations, including Department of Defense Directive 5000.1 and the accompanying milestones, to the acquisition of information technology systems.

(7) The adequacy and transparency of metrics used by the Department of Defense for the acquisition of information technology systems.

(8) The effectiveness of existing statutory and regulatory reporting requirements for the acquisition of information technology systems.

(9) The adequacy of operational and development test resources (including infrastructure and personnel), policies, and procedures to ensure appropriate testing of information technology systems both during development and before operational use.

(10) The appropriate policies and procedures for technology assessment, development, and operational testing for purposes of the adoption of commercial technologies into information technology systems.

(c) **REPORT REQUIRED.**—Not later than one year after the date of enactment of this Act, the Secretary shall submit to the congressional defense committees a report on the results of the review required by subsection (a). The report shall include the findings and recommendations of the Defense Science Board pursuant to the review, including such recommendations for legislative or administrative action as the Board considers appropriate, together with any comments the Secretary considers appropriate.

Task Force Membership

CHAIRS

Name	Affiliation
Vincent Vitto*	Private Consultant
Ronald Kerber*	Private Consultant

MEMBERS

Priscilla Guthrie	Institute for Defense Analyses
Paul Hooper	Private Consultant
Paul Kaminski*	Technovation
Tony Lengerich	Oracle
Noel Longuemare	Private Consultant
Mark Maybury	MITRE Corporation
Richard Roca	John Hopkins University–Applied Physics Lab
John Stenbit	Private Consultant
Alan Wade	Private Consultant

GOVERNMENT ADVISORS

Don Johnson	Office of the Assistant Secretary of Defense for Networks and Information Integration
-------------	---

EXECUTIVE SECRETARY

Skip Hawthorne	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
----------------	--

DSB REPRESENTATIVE

LTC Karen Walters, USA	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
------------------------	--

STAFF

Barbara Bicksler	Strategic Analysis, Inc.
Teresa Kidwell	Strategic Analysis, Inc.

*Defense Science Board member

Presentations to the Task Force

Name	Topic
MAY 19-20, 2008	
Mr. Tim Harp DASD (C3ISR and IT Acquisition)	IT Acquisition/NII
Mr. Josh Hartman OUSD (AT&L)	IT Acquisition/AT&L
Mr. Dave Tillotson Deputy Chief of Warfighting Integration and Deputy Chief Information Officer, U.S. Air Force	IT Acquisition/Air Force
Robert S. Gorman General Counsel, DISA	IT Acquisition Policy and Procedures
LTG Jeff Sorenson Chief Information Officer, Army G-6	Supporting an Expeditionary Army at War
Honorable John Grimes Assistant Secretary of Defense for Networks and Information Integration and DOD Chief Information Officer	Discussion with DOD Chief Information Officer
Mr. Paul Ketrick Business Transformation Agency	Business Capability Lifecycle
Robert J. Carey Chief Information Officer in the Department of the Navy	IT Acquisition/Navy

JUNE 19-20, 2008

Lt Gen Charles Croom Director, Defense Information Systems Agency	IT Acquisition/ Defense Information Systems Agency
Mr. Dave Pratt SAIC	Service-Oriented Architecture Acquisition Working Group
RADM Hilarides Navy Program Executive Officer for Submarines	Rapid Capability Insertion Model
Mr. Don Johnson Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer	Alternative Model in Acquiring Information Technology
Mr. Richard Honneywell Electronic Systems Center, Wright Patterson Air Force Base	Information Technology Acquisition
Mr. Gary Winkler Army Program Executive Officer for Enterprise Information Systems	An Army Perspective on Information Technology Acquisition
Dr. Gary Federici and Mr. Carl Siel Department of the Navy	Law and Policy Implementation Challenges

AUGUST 6-7, 2008

Mr. Roy Evans MITRE Corporation	Rapidly Fielding Information Technology
Dr. Jacques Gansler	Integrating Commercial Systems

SEPTEMBER 16-17, 2008

Dr. Andre van Tilborg Deputy, Office of the Deputy Under Secretary of Defense for Science and Technology	Technology Readiness Assessments as Part of the DOD Acquisition Process
BGen Glenn M. Walters, USMC J8, Deputy Director for Resources and Acquisition Mr. William J. Cooper J8, Capabilities and Acquisition Division	JCIDS and Information Technology Requirements
Ms Regina Begliutti and Dr. Scott Comes Office of the Secretary of Defense, Program Analysis and Evaluation	Analysis of Alternatives Process for IT Systems
Col Ralph W. Harris Operational Test and Evaluation, DOT&E Dr. David Carlson Institute for Defense Analyses	Acquisition of Information Technology – Operational Test Considerations
Clark Reddick Director, C4ISR Technologies David Chaffee Director, Air Force and Agency Programs, Northrop Grumman	Transition to Open Systems
Mr. Gary Pennett Associate Director for Investment Office of the Under Secretary of Defense (Comptroller)	Planning, Programming, Budgeting and Execution Process
Jennifer S. Walsmith National Security Agency Central Security Service Senior Acquisition Executive	Agile Acquisition Process

Glossary

ACAT	acquisition category
AIS	automated information system
AoA	analysis of alternatives
ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
CAE	component acquisition executive
CDD	Capabilities Development Document
CERT/CC	Computer Emergency Response Team Coordination Center
CIO	Chief Information Officer
COTS	commercial off-the-shelf
CVE	Common Vulnerabilities Enumeration
DAB	Defense Acquisition Board
DBSMC	Defense Business Systems Management Committee
DDR&E	Director of Defense Research and Engineering
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODD	Department of Defense Directive
DSB	Defense Science Board
DT/OT	developmental test/operational test
DUSD (S&T)	Deputy Under Secretary of Defense for Science and Technology
EA	economic analysis
EDS	Electronic Data Systems
ESLOC	executable source lines of code
FY	fiscal year
GAO	General Accountability Office
GIG	Global Information Grid
ICD	Initial Capability Document
IOC	initial operational capability

IOT&E	Initial Operational Test and Evaluation
IRB	Investment Review Board
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
ITAB	Information Technology Acquisition Board
JCIDS	Joint Capability Integration and Development Systems
JCS	Joint Chiefs of Staff
JTRS	Joint Tactical Radio System
LOC	lines of code
MAIS	major automated information system
MBD	Milestone Build Decision
MDA	milestone decision authority
MDAP	major defense acquisition program
MDD	Materiel Development Decision
MRAP	Mine Resistant Ambush Protected
MUOS	Mobile User Objective System
NASA	National Aeronautics and Space Administration
NECC	Net-Enabled Command Capability
NII	Network and Information Integration
NMCI	Navy Marine Corp Intranet
NSS	national security systems
NVD	National Vulnerability Database
OASD (NII)	Office of the Assistant Secretary of Defense for Networks and Information Integration
OIPT	Overarching Integrated Product Team
OSD	Office of the Secretary of Defense
OSVDB	Open-Source Vulnerability Database
OT&E	Operational Test and Evaluation
PA&E	Program Analysis and Evaluation
QDR	Quadrennial Defense Review
RDT&E	research, development, test, and evaluation
SDD	System Development and Demonstration

SISOS	software intensive systems of systems
SLOC	source lines of code
SOA	service-oriented architecture
S&T	science and technology
TRA	Technology Readiness Assessment
TRL	technology readiness level
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

234

*Defense Science Board
2006 Summer Study*

on

**Information Management for
Net-Centric Operations**



*Volume I
Main Report*

April 2007

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

The DSB 2006 Summer Study on Information Management for Net-Centric Operations completed its information gathering in August 2006.

This report is UNCLASSIFIED and releasable to the public.

DEFENSE SCIENCE
BOARDOFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

28 March 2007

MEMORANDUM FOR: UNDERSECRETARY OF DEFENSE (ACQUISITION,
TECHNOLOGY & LOGISTICS)SUBJECT: Final Report of the Defense Science Board (DSB) 2006 Summer Study on
Information Management for Net-Centric Operations (Volume I)

I am pleased to forward Volume I (Classified) of the final report of the Defense Science Board Summer Study on Information Management for Net-Centric Operations. Volume II, the Operations Panel Report, which examined the operational value enabled by information networks, will follow shortly.

This study examined the overall conceptual strategy for information operations and the operational value of proposed information networks. Operational scenarios included prevent and protect the United States against catastrophic attack, conduct large-scale counter-insurgency operations including stabilization and reconstruction, conduct global distributed, small-scale operations including counter-terrorism and humanitarian relief, and enable large-scale operations against near peer adversaries.

Observations revealed that complex distributed, ad hoc operations require new information management and command and control concepts. Further, all scenarios require a new information management capability because of the likelihood that a technically capable adversary will attack US and allied information systems. Findings and recommendations conclude that a combat information capability must be treated as a critical defense weapon system, that information assurance must be resourced and its risk managed accordingly, and that an innovative acquisition strategy is required to leverage true commercial off-the-shelf information technology.

I endorse the Task Force's recommendations and encourage you to forward the report to the Secretary of Defense.

Dr. William Schnieder, Jr.
Chairman
Defense Science Board



DEFENSE SCIENCE
BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Report of the Defense Science Board 2006 Summer Study on Information Management for Net-Centric Operations

This Defense Science Board report recommends a new information management approach and combat information capability to respond to current and likely future national security challenges—challenges that require U.S. force to rely increasingly on information, more so than in the past.

For the past five years, the office of the Assistant Secretary of Defense for Networks and Information Integration and the Department of Defense Chief Information Officer have been assembling an underlying framework and architecture based on commercial Internet Protocol technology to address the increased information needs of today's military operations. This enterprise has the potential to bring significant information capability and operational value to users and decision makers at all levels within in the department.

This summer study addressed combat operations, information management, information assurance, and architecture requirements, as well as the architecture framework currently being pursued by the department. The study examined the overall conceptual strategy for the system and the operational value of the proposed information network. Additionally, the task force assessed cost/risk trades and technical network issues such as bandwidth, quality of service, availability, security, integrity for all missions and users, and knowledge management—all of which support the distribution of knowledge that will ultimately support effective decision making. These considerations converged on the simple question of how to provide robust, useful information at all levels—from decision-makers to tactical users.

The findings and recommendations of this study can be distilled to three points

1. the combat information capability must be treated as a critical defense weapon system
2. information assurance must be resourced and its risk managed accordingly
3. an innovative acquisition strategy is required to leverage true commercial off-the-shelf information technology.

The members of the study are greatly appreciative of the important contributions of the government advisors; LTC Scott Dolgoff and Mr. Andrew Chappell, DSB Office representatives; Executive Secretary, Mr. John Mills; and the staff.

Mr. Vince Vitto
Co-Chair

Dr. Ronald Kerber
Co-Chair

Table of Contents

Executive Summary.....	vii
Chapter 1. Introduction.....	1
Chapter 2. Net-Centric Operations and Robust Information Management.....	8
The Problem.....	8
Deriving Major Information Needs from Operational Scenarios.....	9
Operational Gaps.....	11
Current State: Myriad of Ad Hoc Personal Connections.....	12
The Solution: A Combat Information Capability.....	13
Proposed Combat Information Management Support.....	18
Imperatives for Enhanced Command and Control.....	22
Intelligence, Surveillance, and Reconnaissance— an Essential Part of the Combat Information Capability.....	24
Robust Information Management.....	26
Chapter 3. Information Dissemination and Management.....	29
The Technology Context.....	29
System Construct.....	46
Tactical Edge Networks.....	61
Chapter 4: Critical Information Assurance Challenges.....	66
Network/Information Assurance as a Strategic Issue.....	66
Formalized Risk Management.....	67
Threats.....	68
Stratified Network Design.....	73
Chapter 5. A Critical Defense Weapon System.....	80
Operating with Degraded Systems.....	81
Operators Need a System Test Environment.....	83
Operate Effectively with Partners.....	84
Critical Defense Weapon System.....	85
Chapter 6. Conclusion.....	88
Appendix A. Terms of Reference.....	89
Appendix B. Task Force Membership.....	92
Appendix C. Presentations to the Task Force.....	95
Appendix D. Glossary.....	98

Executive Summary

United States national security challenges are much different than they were just a few decades ago. Besides having a much wider spectrum of characteristics and capabilities, potential adversaries have clearly changed and complicated the rules of military engagement to support U.S. security objectives. In “traditional” eras, the adversary was well-defined by lines of battle and clear means of identification. Today’s military operating environment is far more complex: the adversary is dispersed, often mixed with civilians and other non-combatants; and targets are located in areas where there is great concern over collateral damage. Adversaries are adaptive, amorphous, and stealthy, and often do not have high-value targets that can be attacked. The adversaries’ stealth enables them to neutralize the formidable U.S. operational advantages in more traditional warfare, thus making the U.S. reliance on information more pronounced than in past eras.

Over the past five years, the office of the Assistant Secretary of Defense for Networks and Information Integration (ASD [NII]) and Department of Defense (DOD) Chief Information Officer (CIO) have been assembling an underlying framework and architecture based on commercial Internet Protocol technology to address the increased information needs of today’s military operations. This enterprise has the potential to bring the department, at all levels, significant information capability and operational value, and is a valuable defense weapon system. However, the reliance on commercial technology also increases the chances for U.S. adversaries to compromise the enterprise. In response to these challenges, the Defense Science Board was asked to assess the department’s strategy, scope, and progress toward achieving a robust and adaptive net-centric DOD information management system.¹ Specifically, the task force spent time evaluating the current framework, architecture, processes, and organizational structures being

1. The terms of reference for this study are attached as Appendix A.

pursued to deliver the power of information networks to the DOD enterprise, as well as to external partners.

The task force addressed combat operations, information management, information assurance, and architecture requirements, as well as the architecture framework currently being pursued by the department. The task force examined the overall conceptual strategy for the system and the operational value of the proposed information network. Additionally, the task force assessed cost/risk trades and technical network issues such as bandwidth, quality of service, availability, security, integrity for all missions and users, and knowledge management—all of which support the distribution of knowledge that will ultimately support the missions and users in making effective decisions.

These considerations converged on the simple question of how to provide robust, useful information at all levels—from decision-makers to tactical users. The task force focused on support of combat operations, as it was felt to be the most stressing application of the system, as opposed to, for example, business processes and administration. However, it was recognized that all these applications are intertwined and must be operated as a whole. The task force did not examine the protection of the nation's total information network. Although critically important, it was deemed outside the scope of this study.

To set the context of the study, the task force addressed four operational scenarios:

1. Prevent and protect the United States against catastrophic attack.
2. Conduct large-scale counter-insurgency operations, including stabilization and reconstruction.
3. Conduct global distributed, small-scale operations, including counter-terrorism and humanitarian relief (such as Hurricane Katrina).
4. Enable large-scale operations against near peer adversaries.

The task force determined that all these scenarios require a new information management approach and combat information capability for the DOD, largely based on commercial information technology. However, adversaries can access similar capabilities from global commercial vendors. An adversary need not be large in size to capitalize on this capability. In fact, a technically capable adversary can realize a significant military or political advantage by disrupting the information technology supporting U.S. operations—whether or not the United States happens to be directly confronting that particular adversary.

To address this new information management approach and combat information capability, the task force focused on four major themes. Each theme is summarized here and then described in detail in subsequent chapters of this report.

Net-Centric Operations and Robust Information Management Enable Better Decision Making

The task force organized a number of panels of military operators (O-6 level and below) to identify information management needs and how information was managed to execute missions in Iraq and Afghanistan. It became quite clear from these discussions that the United States has considerable deficiencies in its ability to manage information to command and control units in the field.

In the experiences described by the operators, interoperability was poor, and there was significant *ad hoc* activity taking place at the unit level—*especially* at the lowest war fighting echelons. To counter interoperability, U.S. soldiers and Marines developed many systems and processes to move information from one “stove pipe” to another. This included use of personal cell phones sent by family members, chat rooms, web searches, *ad hoc* networks—any solution to get needed information to conduct operations and support commanders. Finally, it was noted that much of the acquired military capability to support these conflicts has been on supplemental funding and is not part of the “planned” system putting into question the long-term viability of these activities.

This *ad hoc* approach also applied during the rotation of units in the field. The task force found that, as operators entered the theater they basically “started from scratch.” Personal, trusted, and comfortable relationships back in the continental United States (“reach-back”) were reestablished. There was ineffective systematic transfer of databases from units exiting in the theater to the inbound units, leading to significant information disconnects as units rotated in-and-out of theater. The inbound unit could not fully exploit the work done by the previous unit. An effective method is still needed for organizing all this information and data, assuring it, and then making it available to the commander to enable intelligent and robust decisions.

Methods for information organization, retrieval, and display are required to enable commanders and soldiers to accurately perceive and understand the information presented to them. Improving a commander’s access to, and understanding of, the information, combined with the ability to collaborate effectively with others, will inevitably lead to better military decision-making.

The task force proposes a combat information management architecture to support the Combat Information Capability (CIC). Three staff functions comprise this architecture:

1. **Combat information specialists.** At-the-ready for the soldier or right beside the commander to answer questions, to anticipate needs, and to assemble and present data.
2. **Knowledge managers.** A reach-back capability for the combat information specialist for information, data, and knowledge in a specific area.
3. **Subject matter experts.** Span a full range of topics and subjects and are the source of in-depth information of a particular subject from which a knowledge base can be assembled and continuously supported.

In addition to the staff functions described above, commanders need to understand, command, control, and operate information management systems at the operational level. Plans to monitor and protect the system, and respond to adversary actions (such as intrusion

or attack), need to be developed. Therefore, the services need to organize, train, and equip information management personnel to develop technological and procedural capability and participate in operational force exercises. Combatant commanders also need planning staff expertise to develop combat information planning annexes to go forward with this system and capability.

Intelligent management of information—whether in the military or civilian sectors—is no longer a choice; it is essential just to keep pace with the competition. Today, several industrial and commercial companies have been very successful at developing this type of organization and management structure, beginning with a lead individual (who also has business accountability) for a wide range of commercial applications and markets. In fact, the very livelihood of companies like large management consulting firms depends on being extremely proficient at this kind of knowledge and information management. The architecture described above basically adapts and institutionalizes best commercial practices to the military.

There are *many* opportunities to improve the current, distributed information management operations in the field. Today's complex distributed, *ad hoc* operations require a new Combat Information Capability to include:

- information management services for tactical users
- dynamic management of distributed intelligence
- intelligence, surveillance, and reconnaissance assets
- appropriate and necessary information assurance and security
- operations with degraded networks
- operations with coalition partners, non-government organizations, other agencies, and state and local governments.

Each of these requirements are touched on in the remaining themes and described in greater detail in the chapters of this report.

Information Dissemination and Management Relies on Global, Interoperable Commercial Information Technology

The information network architecture being developed for the Global Information Grid is based on an Internet-like model with the goal of separating transport from applications. The architecture is supported by a set of net-centric enterprise services, with databases with well-defined ownership and maintenance distributed throughout the network. Implicit in this architecture is: (i) a robust core at the transport level; (ii) a useful set of services; and (iii) a robust set of ever-increasing applications, as communities of interest are organized to define those applications. The services and other users must develop key applications, but in a manner that decouples the applications from the individual databases.

The task force was briefed on a number of the programs: Global Information Grid Bandwidth Expansion, Transformational Satellite Communication, Joint Tactical Radio System (JTRS). It was not the intention or the purpose of this task force to focus on the schedule, acquisition strategy, or technological issues associated with each of these programs. The task force however did consider two programs very important to information management and assurance. They are Net-Centric Enterprise Services (NCES) and High Assurance Internet Protocol Encryption (HAiPE).

Overall performance of the system can only be assured by developing a comprehensive model of the system, and testing additions and modifications with a systems engineering approach. Such an approach requires high-level analysis, as well as detailed systems modeling, to guide evolution of the system. The implications of programmatic and configuration changes within the overall system must be assessed, as well as information assurance weaknesses. The objective of this approach is to develop and monitor performance metrics, and to develop the capability to test the systems and applications for compliance with performance objectives.

Finally, end-to-end testing and technical control are imperative to stress the network for technical and operational parameters, as well as to understand and measure the formal risk management processes trading performance versus assurance. This system is being built predominantly with commercially available information technology, so new information assurance vulnerabilities are introduced as new capabilities are added.

The DOD does not have adequate resources within the offices of the ASD (NII), CIO, the Defense Information Services Agency (DISA), or the Under Secretary of Defense for Acquisition, Technology and Logistics (USD [AT&L]) to perform comprehensive systems analysis and engineering. While the task force believes the workforce should be improved, it was struck by the paucity of involvement of commercial experts in this needed systems analysis area. The task force believes experts from commercial industry be brought in (perhaps on short-term Intergovernmental Personnel Act tours) to assist the acquisition and systems engineering processes, and to identify commercial activities that could be brought to bear on the DOD enterprise.

As the task force surveyed the entire enterprise architecture and assessed the proliferation of commercial information technology, it was recognized that, although much focus has been placed on commercial-off-the-shelf (COTS) technology, it often means “enhanced COTS” or “value-added COTS”—that is COTS technology that has been modified by a large systems integrator. The DOD is already buying routers, switches, blade servers, and software directly from the General Services Administration catalog. So, a great deal of the information technology already in this system is true commercial information technology—in fact, the department is encouraging commercial instantiations of new information management and assurance approaches (e.g., HAIPE and NCES). However, the department currently uses the Joint Capabilities Integration and Development System (JCIDS) process that is designed for large-scale, requirements-driven acquisitions—a process that leads to “enhanced COTS” or “value-added COTS.” A capability-driven approach is needed to develop and inject information technology components into the information enterprise.

Although the discussion above defined a Global Information Grid (GIG) core network supported and protected by HAIPE security devices, at the edge of the core are many tactical networks that can assume many forms, e.g., coalition, special operations, Army, Marines. To accommodate the information needs of the tactical user, the edge networks must support a minimum standard interface back into the GIG core. Since the users and operators in the edge networks are the ones who identify the information needed to carry out their mission; they should be able to pull that information from the databases within the system, using the common services provided by NCES.

The central problem identified by the task force is that the information needs of tactical users and edge networks are not being adequately addressed. The current focus is on communications—not on information management needs. Combat decision support tools are needed to provide reach-back, combat information, and database management. Commander's expectations must be managed within these tactical networks.

In addition, tactical communications devices being developed within the JTRS and other Service programs will not allow tactical users to keep up with the revolution in commercial wireless technology. Unique approaches are required to provide tactical users with inexpensive information management devices.

Commercial Information Technology Architecture Presents Critical Information Assurance Challenges

Information assurance is an enormously important issue: information assurance enables mission assurance. Information assurance is typically treated as if it were a network security and confidentiality matter. Yet it actually entails several additional issues, including integrity of the system, availability, quality of service, authentication, and attribution.

With the addition of each new module of capability, a degree of vulnerability is added. The clear need is for a formal risk management process that considers obvious benefits of net-centric operations along with the information assurance threats that are not as intuitive.

A formal risk management process needs to be embedded in the systems engineering and analysis processes, to assess the benefits of added applications against the impact of the introduced information assurance threats. There are many other potential threats in DOD networks, including offshore development of hardware and software. The information network is inherently vulnerable, and it needs to be designed and operated with the understanding that it is or can be attacked and/or compromised.

Use of a COTS-based information network is critical to keep the system capabilities close to those that are commercially available. *Yet, this is the first major U.S. defense system that is built on commercial, globally available technology.* This strategy therefore inherently raises the risk that adversaries can also exploit commercial technology. It also means that the system is more difficult to protect, especially as additional capabilities are added. COTS on the scale proposed will enable a system more robust than anything an adversary will likely assemble, but use of COTS is inescapably a double-edged sword from the information assurance perspective, because the high speed of COTS implementation may outpace the ability to maintain integrity and control of the system itself. This is why the provenance of the hardware and software being inserted into this system must be carefully monitored. Globalization and off-shore development greatly increases this threat. A three-prong strategy is needed for dealing with information assurance matters: an offense component, a deterrence and dissuasion component, and a defense-in-depth component.

“Combat Information Capability” is a Critical Defense Weapon System

At the start of this study, members thought the task force would focus on information management issues, the GIG, and a myriad of other technical issues, but as briefings were received from users, operators, and experts, concepts and thinking about this subject transformed. This system will touch and manage all DOD information resources, especially those in time-critical battle situations, and it needs to be treated as a critical defense weapon system. As a weapon system it

must be protected and operated in a manner consistent with its mission of protecting and defending the United States.

A critical defense weapon system requires enterprise-wide operational management, performance monitoring, and contingency planning functions. Operators must know how to operate the combat weapon system, and readiness assessments, throughput and performance, and trades and metrics to measure both performance and assurance must be available. Many defense assets will be connected via this system and system services must be prioritized and tested, and war fighters must train with the system.

The system will likely always be operated in a degraded mode and the assumption should be that adversaries are constantly attacking it. As a defense weapon system, doctrine; concepts of operations; tactics, techniques, and procedures; and contingency plans must be developed to address these threats. The system must be exercised regularly—with employment of deception—so U.S. commanders understand how to operate in degraded modes. Calibrated red and blue teams can be used to help with scenarios and develop exercises that are realistic. Commanders must be provided the necessary network status information to make risk-managed decisions about the mode of operation—such as available capacity or estimated extent of penetration.

A system test environment is needed for enhancements, assurance modifications, and new commercial capabilities to be tested before being inserted into the real system. In such an environment, red team attackers and blue team defenders can exercise solutions or offerings and improve skills without impeding actual operations. Ideally there should be several test range options, ranging from virtual (rapid simulation of applications and capabilities being considered for incorporation into the network system), to simulation (table top experiments), to live exercises (calibrated red/blue teams to introduce real-world system characteristics). Ultimately, live field exercises should be conducted to understand how to manage and protect the system realistically and effectively.

Recommendations

The task force proposes the following recommendations that cut across the four themes identified above, to develop the necessary strategies, policies, training, and countermeasures to use, protect, and manage this defense weapon system.

1. The Department needs to recognize information capabilities as a combat system.

- Deputy Secretary of Defense should create and resource a Combat Information Capability
- United States Strategic Command (STRATCOM) must improve net-centric operations:
 - Joint Task Force Global Network Operations center must be improved to a world-class enterprise management capability.
 - Performance and readiness metrics must be developed.
 - Network management standards must be enforced across the enterprise.
 - Robust and redundant capabilities and operational procedures for information assurance must be developed.
- STRATCOM must establish a robust GIG test environment to examine the trades among performance, information assurance, and cost:
 - DOD CIO: Identify and prioritize emerging information technology and information assurance capabilities for testing.
 - U.S. Joint Forces Command (JFCOM): Create net-centric operations and information assurance learning and training experiences.
 - Combatant commanders: Conduct operational readiness exercises and tests.
 - STRATCOM, National Security Agency, and DISA: Validate and exercise a risk management system.

- STRATCOM and JFCOM: Identify resource requirements.
- Chairman, Joint Chiefs of Staff must develop a Combat Information Capability Strategic Plan

2. *Combat Information Capability requires a new approach to information management.*

- Deputy Secretary of Defense should direct DOD CIO to ensure the formation of communities of interest. These communities should be aggregated into capability portfolios to rationalize vocabularies and harmonize services and value-added services.
- Deputy Secretary of Defense should direct DOD CIO to ensure DOD process owners encourage creation of an information marketplace to include:
 - Delivering value-added services.
 - Developing resource incentives for making data visible and promoting information sharing.
 - Developing processes to ensure information quality.
- Deputy Secretary of Defense should direct the services to create and resource combat information positions to include:
 - Combat information support staff, combat information specialist, as well as knowledge managers and subject matter experts.
 - Provide commanders at 3- and 4-star level with combat information integration officers on their personal staffs.

3. *Create an enterprise-wide, robust information assurance strategy.*

- ASD (NII) should evaluate the information assurance funding over the Future Years Defense Program, focus on information assurance for the entire enterprise, and increase current funding where appropriate.

- DOD CIO and ASD (NII) should establish responsibilities and authorities for overall enterprise governance.
- DOD CIO and ASD (NII) should develop a robust systems engineering and risk management capability.
- ASD (NII) and USD (AT&L) should establish a defense-wide program to design, build, and operate an isolated network to improve GIG information assurance capabilities.
- DOD CIO, ASD (NII), and USD (AT&L) must establish plans, policies, and procedures for acquisition of COTS information technology systems from an information assurance perspective.
- USD (AT&L) and ASD (NII) must address critical programmatic issues with NCES and HAIPE.
- STRATCOM and JFCOM should devise an information assurance battle management doctrine, and tactics, techniques, and procedures.

4. *Combat Information Capability must support tactical communications and leverage COTS information technology.*

- USD (AT&L), DOD CIO, and ASD (NII) should support the tactical users at the edge of the core by:
 - Delivering robust, easily formed, meshed tactical networks that leverage commercial technologies.
 - Delivering information that adapts to tactical users display and bandwidth.
 - Implementing robust content staging to provide information caching forward to enable timely access.
 - Encouraging the production of future commercial capabilities that meet the department's needs.
 - Acquiring end-user devices as commodities, through the General Services Administration Schedule.

- Chairman, Joint Chiefs of Staff and USD (AT&L), should revise JCIDS and acquisition system policies to encourage rapid information technology procurement and to:
 - Exploit opportunity to purchase COTS information technology, which will require spiral acquisition processes.
 - Assure COTS systems remain true COTS with plug and play interfaces.

The bottom line: this Combat Information Capability must be treated as a critical defense weapon system, information assurance must be resourced and risk-managed accordingly, and an innovative acquisition strategy is required to leverage true COTS information technology.

Chapter 1. Introduction

The military's ever increasing reliance on information networks and its ability to provide wider access to information to support collaboration has transformed and improved the forces' capabilities and effectiveness in executing operations. Future challenges and the need to maintain adequate levels of security, integrity, and reliability will place new demands on information networks, processes, and personnel. The Defense Science Board was asked to assess the department's strategy, scope, and progress toward achieving a robust and adaptive net-centric information management capability for the Department of Defense (DOD).

It is well accepted that improved information at all levels will improve operational effectiveness, but, of course, that comes with some risk and penalties. The task force was asked to examine the operational value of the proposed information network and to pay special attention to the emerging missions it is designed to support—that is, counterinsurgency, counterterrorism, stabilization and reconstruction, response to catastrophic disasters, and defense of the nation against attack.

Over the past five years the Assistant Secretary of Defense for Networks and Information Integration (ASD [NII]) and Chief Information Officer (CIO) organizations within DOD have done a significant and remarkable job assembling an underlying framework and architecture based on commercial Internet Protocol (IP) technology, which has the potential to bring the department, at all levels of the enterprise, significant information capability and operational value. The task force was charged with evaluating the framework, architecture, processes, and organizational structures being pursued to deliver the power of information networks to the DOD enterprise, as well as to external partners.

Risks are associated with execution of programs to implement the network, as well as with meeting quality of service, availability, security, and integrity expectations for all missions and users. The task force was to assess cost/risk trades and technical network issues associated with the enterprise.

Lastly, the task force considered knowledge management in support of department goals. “Googling” for access to particular information is now a familiar activity, but it is not the appropriate application for the war fighter in the tactical battlefield who is seeking information in the middle of a firefight. Therefore, identifying effective methods to provide robust, useful information at all levels—from strategic decision-makers to the tactical user—was a major focus of this study. The focus would be on information discovery, sharing, collaboration, visualization, comprehension, and storage—all of which support the distribution of knowledge that will ultimately support the missions and users in making effective decisions.

The following operational scenarios derived from the threat assessment prepared for the most recent Quadrennial Defense Review were the basis for the task force:

- prevent and protect the United States against catastrophic attack
- conduct large-scale counter-insurgency operations including stabilization and reconstruction
- conduct global distributed, small-scale operations including counter-terrorism and humanitarian relief
- enable large-scale operations against near peer adversaries

As depicted in figure 1, these scenarios today have a very different battle management paradigm with a stealthy enemy dispersed in a civilian urban setting, as opposed to clearly defined, uniformed combatants and battle lines for engagement as in previous wars.

Under all scenarios a sophisticated and “state of the art” information management capability is required.

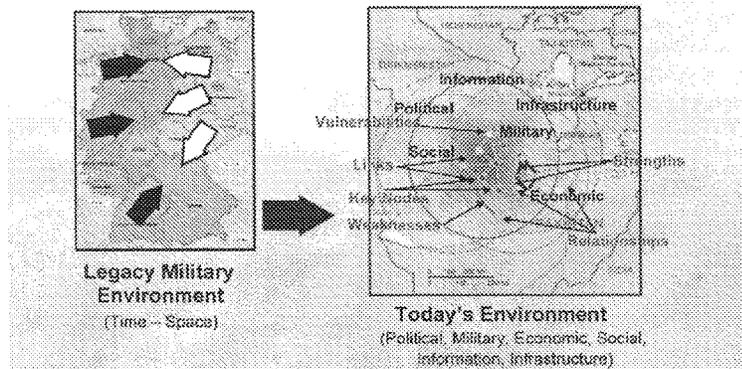


Figure 1. Evolving Threat Drives Need for New Combat Information Capability

Information systems technology has proliferated across the globe, driven primarily by the global economy and the Internet. The United States no longer holds a significant advantage in information systems technology. Today, more hardware and software is being built offshore than in the U.S., and that percentage continues to grow rapidly. Potential adversaries are technically very capable and are able to move information rapidly. Adversaries also clearly understand the importance of information to winning in combat and will therefore commit themselves to attacking U.S. command and control, communications, and information systems. These attacks may be kinetic attacks and/or non-kinetic attacks. The threat to the information system will continue to evolve as globalization and the information revolution force changes in structure and technology.

In our lifetimes, the information revolution has moved the world from a place where data can be moved at about 30 words per minute over field phones and 60 words per minute over radios to one in which it can be moved at roughly 1.5 *trillion* words per minute over wideband data links. At the same time, data acquisition through means such as satellites and data storage capabilities has increased at a similar rate. The impact of this revolution on information management capability on the national security environment is enormous. It would be especially detrimental if

there is not a U.S. national and DOD commitment to keep pace with almost “speed of light” advancements in information technology.

Globalization has radically changed the national security paradigm. Movement has been from a relatively isolated environment of the Industrial Age of the 20th century, where security meant “defense” and “containment,” to the information age of the 21st century, a much more integrated environment with a smaller world (due to speed of light transmissions) where information is shared globally in very near real time, and national security is more complex and dynamic. Maintaining “national security” is no longer just a matter of protecting international borders. For example, “borders” in cyberspace must also be protected.

At the same time, there are more active global hotspots; the threat is increasingly using asymmetric tactics; and interoperability is still an issue with U.S. forces, as well as with many of U.S. coalition partners. The evolving threat characteristics considered during the course of the study include:

- dynamic and ever changing
- highly mobile and regularly move across international borders
- highly distributed
- stealthy
- adaptive and amorphous
- asymmetric
- when viewed in isolation—low value targets

Adversaries have become very skilled at neutralizing U.S. operational advantages. Two critical concerns evolved during the study:

1. U.S. adversaries are not only using their many skills in information technology to move information rapidly, but also they may develop a significant capability to attack U.S. information systems.
2. Commercial-off-the-shelf (COTS) information technology production—both hardware and software—is moving to Asia.

The implication of this trend on national security is alarming.

It should be noted that since Operation Desert Storm, the United States has reduced the size of its war fighting forces by 300 ships, 12 air wings, and 6 divisions. With a modernization budget that has essentially remained level and/or declined, the department has invested heavily in information technology; networks; precision; command, control, and communications; computers; and intelligence, surveillance, and reconnaissance (ISR). Essentially, the United States is engaging in a fundamental trade of massed forces for massed electrons. This trend has focused toward a capability to more precisely and surgically attack smaller units down to a single terrorist.

During its deliberations, the task force identified four major themes:

- Better military decision making (all echelons, all missions) is enabled by net-centric operations and robust information management.
- Information dissemination and management relies on global, interoperable commercial information technology.
- Commercial information technology architecture presents critical information assurance challenges.
- Field and operate a Combat Information Capability as a critical defense weapon system.

The findings and recommendations in this report are formulated around these themes.

While many of the implications of this task force's findings would also apply to, for example, management of administrative or financial systems within the DOD, the task force chose to build this study around the last theme because the combat environment is the most *stressing* application.

The task force defined a Combat Information Capability (CIC) as the ability to manage information and information sources to support commanders at all levels in any type of confrontation with an adversary to deliver the best data *to the last tactical mile*. This capability is built on a foundation that includes all the services on the Global Information Grid (GIG), information assets, databases, capabilities to manage information, and the ability to protect the GIG and its assets. These assets are brought together with real-time information, such as ISR data gathered from all sources. *This Combat Information Capability is an integration of assets, capabilities, applications, and databases that all work together to enable timely smart decisions in the field.*

Due to the enormous scope of this subject, the task force had to exclude many important subjects from consideration. While the members recognize that many “outside” networks are attached to the DOD infrastructure, this task force chose not to undertake the impact of an attack on national infrastructures outside the DOD networks. However, there must be protections on information that enters the DOD system from those outside networks.

The Bottom Line

As the task force evolved, it became clear that, given the way this system is to be fielded, *the Combat Information Capability must be treated as a critical defense weapon system* that will provide a great deal of capability to the United States. With this realization, a different mindset is required on how the system is used, managed, and protected.

The evolving national security scenarios demand increasingly distributed and dynamic operations. The network/COTS approach and strategy certainly enable new paradigms for sharing and using information. However, this capability also has the potential to significantly *increase* vulnerabilities to internal and external threats. It becomes a very attractive target for U.S. adversaries.

Therefore, the task force believes that the system and its capabilities have the potential to be under attack and, as a result, commanders must be prepared to operate in either a degraded or compromised mode.

Commanders need to understand this potential and be trained to operate under this scenario.

A major implication of the network/COTS approach is that DOD needs a new, innovative acquisition strategy so that full advantage can be taken of the capabilities of a true COTS system.

The task force's findings and recommendations can be distilled to three points, which will be repeatedly visited in the following chapters of this report:

- **DOD Combat Information Capability must be treated as a critical defense weapon system.**
- **Information assurance for this critical capability is critical and must be resourced and risk-managed accordingly.**
- **An innovative acquisition strategy is required to leverage true COTS information technology.**

Chapter 2. Net-Centric Operations and Robust Information Management

The Problem

The focus of most combat operations in the past several years has been overwhelmingly in the land domain. The distinguishing characteristic of this domain, with some exceptions, is its people-centric nature. This is distinct from the platform-centric nature of other domains or even more traditional conventional land combat warfare. The recent experiences of war fighters in the tactical environment, employing the currently fielded net-centric capabilities, provides the department a critical opportunity to validate the theory and promise of information management and networks at the tactical level. The power of information and accurate battlefield situational awareness is as old as conflict and warfare itself. The distinguishing difference between now and all of history is the explosion of information management and communication technology in this information age.

This rapidly developing technology presents many different challenges than our most recent differentiating defense technologies (nuclear weapons, submarines, fighter aircraft, stealth, and precision weapons), and, most importantly, is in the commercial sector. The fact that most of the technology is globally and commercially available means that U.S. adversaries can exploit it as rapidly as the United States can. This in fact implies that it would be very risky for the United States not to exploit the technology as rapidly and as prudently as possible. The validation of the network-centric operations (NCO) thrust of current DOD activities should also include a serious look at the risks, vulnerabilities, and challenges introduced by using this technology.

War fighters are singularly focused on capabilities that help them achieve their assigned missions. Sophisticated information capabilities introduced in the past several years have made a significant impact on the tactical battlefield. On the positive side the ability to share, communicate, and collaborate using vast amounts of information is changing the way

some commanders organize forces for combat. On the negative side is the continuous *ad-hoc* nature to tactical networking solutions. In some cases, the solutions to capability shortfalls are solved by adapting commercial capabilities outside programs of record. In other cases it is adapting programs of record through the use of civilian networking concepts like web chat.

The task force heard from four panels of operators at the O6 level and below who had just returned from Afghanistan and Iraq. Their observations varied according to their particular experiences but several themes can be easily summarized to a few critical issues. Information management was the war fighter's principal concern. Finding the needed information effectively and in a timely manner was very difficult for the tactical commander and staff. The information management challenge at the tactical level was couched in very practical terms: the war fighters want information management concepts that support, not restrict, concepts of operation. Commanders want improved access to ISR data and tasking plans at the tactical level. In some cases, this access is desirable without value-added analysis; in other cases intelligence processing is helpful as long as it is timely. Establishing information sharing and collaboration seamlessly for voice, data, and video without regard to organizational echelon is the desired end-state.

Deriving Major Information Needs from Operational Scenarios

The four operational scenarios developed during the Quadrennial Defense Review were examined to comprehend the major information needs for combat or crisis management operations.

When the four operational scenarios are examined in detail, certain major information requirements become clear for each scenario. These information requirements include data, communication and collaboration capabilities, and tools that would facilitate success in each of the respective scenarios. These needs are by no means exhaustive, but the ones listed below and shown in figure 2 are illustrative for the respective scenarios and they provide a good sense of the types of information required for today's security challenges.

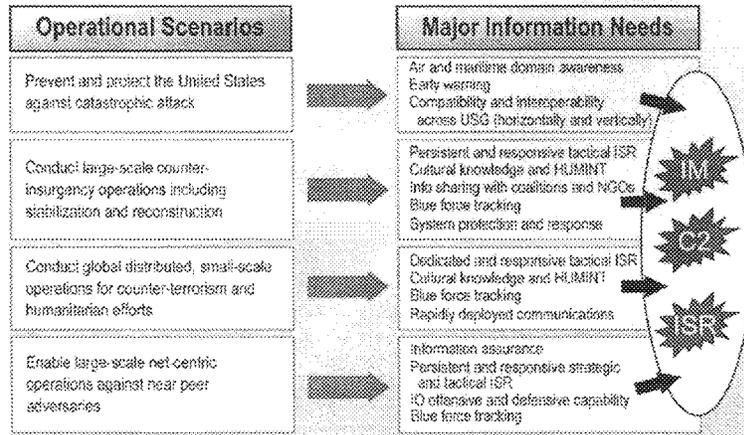


Figure 2. Assessing Combat Information

The examination of figure 2 shows that even with significant commonality across the scenarios, the major information requirements have some distinct needs for each operational scenario. Nonetheless, three major areas emerge as central throughout all scenarios:

1. Information management (IM)
2. Combat Information Capability command and control (C2)
3. Intelligence, surveillance, and reconnaissance

Moreover, information management, command and control, and ISR—taken as a whole—combine to form what the task force termed a “Combat Information Capability,” a term that will be defined and developed in the subsequent discussion. There are significant capability shortfalls in these areas that need to be addressed. These gaps will also be discussed below.

Operational Gaps

Recent operations have re-enforced the endemic challenges of providing the right information at the right time in the right form. The ability of commanders to organize and manage information and related resources was limited by a host of complex interrelated issues. The most common refrain was visibility, access, and flexibility. In general, there is a significant gap in the ability to manage combat information, which includes the process of identifying, collecting, organizing, making available, assuring quality and authenticity, and protecting information, for operational use. Emerging information management techniques will provide essential mission functionality for the user to discover data and services, to understand and use information, and to collaborate with other users.

The second category is in the area of command and control within the scope of activities generally associated with information collection and management. Commanders at all levels recognize the necessity to understand the critical capabilities necessary for mission success. Many of the war fighters realize that “control” of assets is not the crucial issue. The challenge is a fundamental lack of ability to see, understand, and influence critical issues such as bandwidth, ISR management, and information sharing with coalition partners.

The third major area of concern from the tactical war fighters was the inability to access or fuse ISR data. The ISR data being referred to most often was in the form of imagery intelligence but would include the full range of sensor outputs to include human intelligence (HUMINT) reporting.

The often repeated statement “every soldier is a sensor” is meaningless unless the flow is two way and accounts for the nature of the environment in which the information is useful. Data collected at and for the ground tactical level (complex physical and human terrain) is by its nature incredibly cluttered. The nature of operations in this environment (ambiguity, time sensitivity and constraints, mobility) means that the sensors generally tell a commander less and less precisely than for example when compared to platform-centric environments.

Current State: Myriad of *Ad Hoc* Personal Connections

Information management is the process of identifying, collecting, organizing, making available, assuring quality, and protecting information for operational use. Information management provides essential mission functionality for the user to discover data and services, understand and use information, and collaborate with other users. This task force focused on the use of information management in support of military operations and combat information management, which is believed to be the most stressing application of the DOD information management strategy. The task force did not directly examine DOD business or administrative systems; however, some of the principles identified in this task force directly apply to those applications, e.g., true COTS and streamlining the acquisition process.

Unfortunately, current military operators are not enabled with a robust and world class combat information management system. Currently, combat information support is provided by a myriad of *ad hoc* personal connections that are established each time units rotate into theater, only to be broken when they rotate out. The scenario depicted in figure 3 shows a typical unit's *ad hoc* reach-back approach to comfortable and familiar sources.

Combat information management promises a number of benefits of including:

- More responsive and informed decision making—owing to more rapid and wider information sharing and enhanced presentation. This can provide forces with greater flexibility to adapt to unanticipated circumstances.
- Improved situational awareness—drawing on wider information sources and shared understanding (such as Command Post of the Future²).

2. <http://www.isx.com/projects/cpof.php>

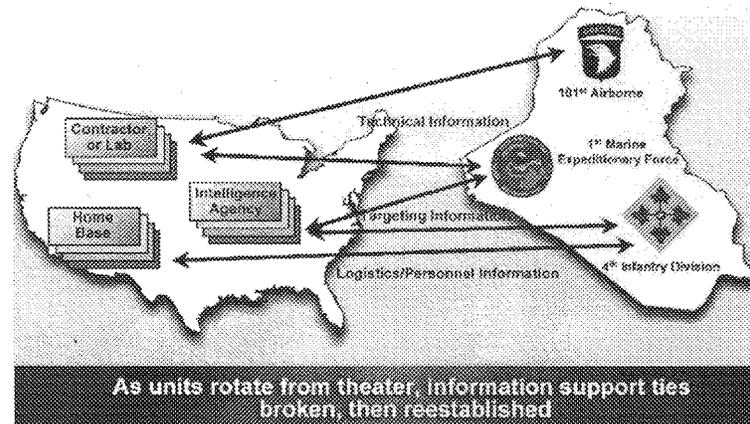


Figure 3. Current Status—Myriad *Ad Hoc* Personal Connections for Information Management Support

- Enhanced and timelier planning—resulting from greater collaboration and increased parallel activity. This can include the ability to operate with a smaller footprint forward as illustrated in the forward Air Operations Center in Joint Expeditionary Force Experiments.
- Improved synchronization in mission execution—resulting from increased coordination among distributed forces that can result in more rapid and effective operations and lower fratricide.

The Solution: A Combat Information Capability

The Combat Information Capability can best be described by referring to figure 4. The foundation is the Global Information Grid extended to the High Assurance Internet Protocol Encryptor (HAIZE) including information assurance elements of the Net. This design provides wideband capability with robust defenses. The elements involved in protecting and assuring the net assume that adversaries will attempt to deny this important capability. The information assets refer to data that are generally stored in data bases and sources available to the

war fighter. Sensor data, track data, and analysis of information would fit into this characterization.

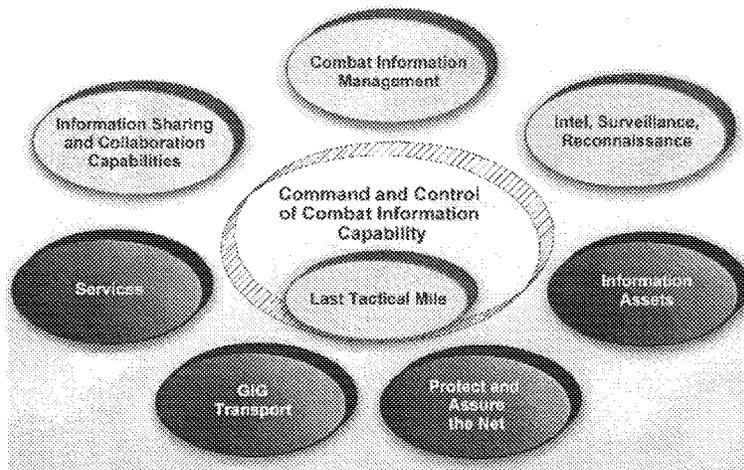


Figure 4. The Combat Information Capability

Services are the tools that permit discovery and exploitation of data, applications, displays, and persistent collaboration capability to satisfy combat information needs. These four elements are part of the CIC. Depending on the scenario, the GIG, the information assets, the services and protect/assure parts of the foundation can be separated from the normal business of the department to attain a higher priority, greater assurance and security, and more secure data bases and services by parsing.

The gray areas in figure 4 are focused on the operational and tactical level of operations and the recommendations to improve capabilities over the last tactical mile. The “last tactical mile,” which generally lies outside the secure HAIPE protected core of the network, may have limited communications bandwidth, has unique security and assurance requirements and challenges, and warrants particular focus in this study.

The necessary requirements to support the “disadvantaged” war fighter are outlined later.

Combat information management refers to the process and structure to provide commanders and individual war fighters with educated and trained assistants and tools to understand and support combat information requirements. An information sharing and collaboration capability refers to the tools and communications that provide commanders and staffs the ability to share information dynamically and to collaborate for planning and execution. Command Post of the Future capabilities in Iraq are an excellent illustration of the value of collaboration. The ISR element refers to the ability to treat operational and tactical ISR assets as an integrated ISR “system” to obtain the most effective, responsive coverage from available assets. The data flowing from ISR assets may be made available simultaneously to the user and to the analyst.

To achieve maximum combat effectiveness, the commander must be able to control this war fighting capability as is done with other essential elements of combat power. The task force defined the needs that permit the commander to exercise command and control.

Taken together, these seven elements comprise a CIC.

Organizing Data for Robust Decisions

Command centers at both the strategic and operational levels, as well as tactical joint force elements, must have a common understanding of the location and identification of all battle space entities (that is, people, air vehicles, ground vehicles, ships, subsurface vehicles, space vehicles, buildings, bridges, and critical infrastructure components, for example). This information comes from a variety of sources, many of which are represented in the ovals on the left side of the figure 5. Under the concept of a net-centric force, it is envisioned that these sources will be networked and integrated together in such a manner that precise tracking and identification of all battle space entities will be achieved. It should be noted that some key work is already underway in the department under the auspices of the Joint System of Systems Engineering Office to integrate sensor inputs to

achieve unambiguous air track data so that a single integrated air picture can be created. Experts advise that the same software engineering approach that is being employed to create an unambiguous air track data environment can also be employed for the other domains (land, maritime, space, and perhaps cyberspace), thereby creating an unambiguous track data environment for all domains.

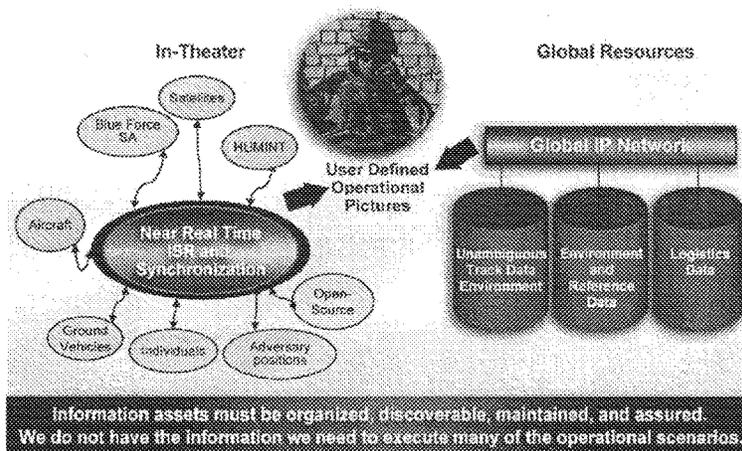


Figure 5. Organizing Data for Robust Decisions

This unambiguous track data environment created primarily via a well-synchronized, near real-time ISR tracking network (illustrated in figure 5) will then become a key information source that can be shared across all joint force elements via the GIG. The information from this key CIC data source, as well as information from the other data sources shown above, can then be displayed by joint force elements (users) in many different ways and on varying scales via user-defined operational displays. The displays needed at the tactical level may vary significantly from those required in a command center; however, the important premise that must be accepted and followed is that all user displays must use common data sources so that the information is consistent and authoritative across the entire joint force. A conceptual representation is depicted in figure 6.

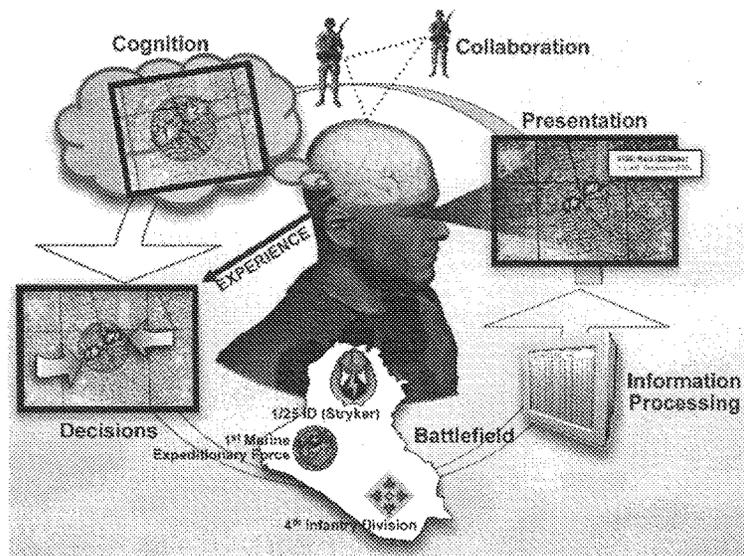


Figure 6. From Data to Effective Decision Making

Once the information is made available to the user, the next major problem to address is how to support that user in understanding the information. The solution lies in net-centric operations theory as articulated by, among others, Garstka and Alberts.³ This theory addresses:

- The physical domain where strike, protect, and maneuver takes place across the environments of ground, sea, air, and space.
- The information domain, where information is created, manipulated, value-added, and shared. It can be considered the “cyberspace” of military operations.

³ Network Centric Warfare, August 1999, David S. Alberts, John J. Garstka, and Frederic P. Stein; “Power to the Edge,” June 2003, David A. Alberts and Richard E. Hayes

- The cognitive domain, where the perceptions, awareness, understanding, decisions, beliefs, and values of the participants are located. These intangibles are crucial elements of network centric operations.
- The social domain, where force entities interact, exchanging information, awareness, and understandings, and making collaborative decisions. It overlaps with the information and cognitive domain but is distinct from both.

Cognitive activities by their nature are individualistic; they occur within the minds of individuals and are, therefore, the heart of decision making. These concepts can be applied to design of displays and training modules to enhance perception and understanding of all war fighters.

Proposed Combat Information Management Support

Combat information management involves the seamless, timely flow of information between and among a globally connected set of partners. The task force concludes, however, that commanders and tactical level combatants will need assistance in managing critical information needs until better information management tools can be created in the future. Thus, it is recommended that new skill sets be created called combat information specialists augmented by knowledge managers and subject matter experts. The details of all three are discussed below and the proposed information management architecture is shown schematically in figure 7.

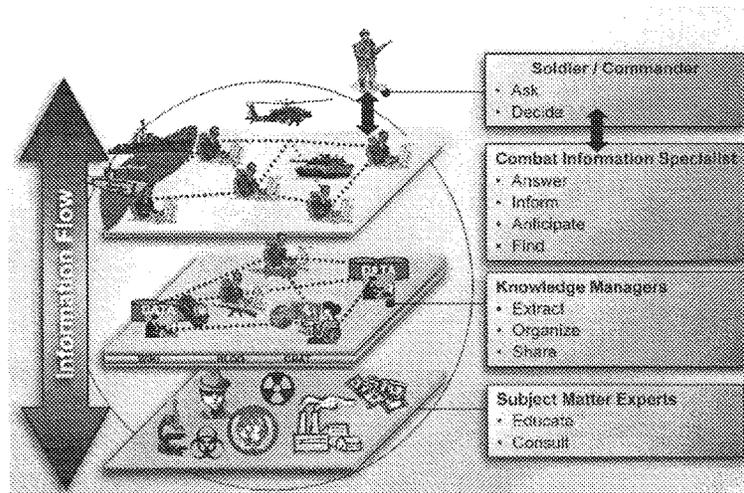


Figure 7. Proposed Combat Information Management

To date there has been an overall lack of focus and effort on managing information in the GIG—its creation, quality assurance, access control, and timely and appropriate dissemination. The private sector, especially those involved in businesses where a “knowledge advantage” provides a critical competitive edge, recognizes the value of information and invests in systems and people to exploit it. For example, Accenture (Accenture.com), a \$15 billion global management consulting and technology services company, recognizes that their information base and experience is their most valued corporate asset and they treat it as such. They assign more than 150 information managers (called knowledge managers) to functional specialties such as oil, gas, insurance, and pharmaceuticals.

Information managers collect, process, and store for dissemination to interested parties the latest and most important information in their domain. They know the most relevant sources, the best subject matter experts, and identify the best practices in their focus area. They are responsible for both quality and content of information in their domains. They ensure that the full company’s knowledge base is

available to all company representatives who interface with customers. Their focus is on the information and its management, not on the technology for its storage and delivery—though they rely heavily on an effective technical base. Typically these managers are also practicing consultants that organize the knowledge and ensure all newly collected or generated knowledge by anyone in the company is systematically added to the database.

Current DOD doctrine does not explicitly recognize the management of combat information as a critical military resource. Accordingly, both services and combatant commanders need to create combat information positions and associated concepts of operations. Figure 7 illustrates roles and example responsibilities of key players in a proposed approach to the provisioning of combat information management. In that proposed approach, combat information management support ranges from near-real-time intelligence (such as provided by combat information specialists) to longer-term substantive analysis (such as provided by knowledge managers and subject matter experts).

In particular, the creation of three distinct levels is recommended. At the first level, closest to the operator in space and time, combat information specialists answer, find answers to, and anticipate questions from commanders and operational users in the field. In developing answers to those questions, they may collaborate with combat information specialists supporting other units and commanders and/or they may work with knowledge managers who identify, discover, extract, organize, catalog, and maintain information about a selected set of topics. Knowledge managers, and others, use subject matter experts, who provide in depth knowledge, advice, and consultation in highly specialized areas.

Effective combat information management will require further refinement of roles and responsibilities, as discussed below. It will require development of concepts of operations and staffing plans. It should build on current service and combatant command efforts in this direction, as well as intelligence community assets. Success will require dedicated and trained staff at multiple echelons, although in many cases this will be possible through the redefinition of existing staff. A primary result will be

seamless, persistent, expert information support as units rotate in and out of the theater.

Combat Information Specialist

Combat information specialists answer operational requests, anticipate and track operational information needs, and disseminate critical information to combatants, both in mission rehearsal/preparation and in real-time support of mission execution. They are integrated into units at all echelons, have intimate understanding of the unit's missions and objectives and, as such, are essential elements of the unit fighting team. They have access to classified information typically at the SECRET level, and possess an extensive network of contacts for information and intelligence. They share information with peers in the combat theater, can act as information liaisons with coalition forces, and provide knowledge managers with assessments of the value of information, as well as after action reviews, which knowledge managers will assimilate into their individual domains as appropriate. This skill is envisioned as a military occupational specialty.⁴ In fact, the Air Force has defined an information manager specialty.⁵

Knowledge Manager

Knowledge managers are responsible for obtaining, organizing, maintaining, and sharing operational and technical knowledge in a specific focus area. For example, there might be knowledge managers focused on improvised explosive devices, surface to air missiles, Islamic culture, regional economics, or regional politics. While they are not necessarily subject matter experts, they need to have knowledge of the best sources of information and possess an extensive network of expert contacts. While they need not be physically collocated with operators, they are intimately aware of operational concerns and discover operational insights via their interactions with combat information specialists and users. One key role they play is as arbiters of quality.

4. See: http://en.wikipedia.org/wiki/Military_Occupational_Specialty

5. See: <http://usmilitary.about.com/od/airforceenlistedjobs/a/afjob3a0x1.htm>

Services provided by knowledge managers are shared across units, with dozens initially deployed, growing to hundreds at steady state, dynamically altering according to changing information needs. Knowledge managers are experts in a particular area and they are drawn from a variety of military skills.

Subject Matter Experts

Subject matter experts possess in-depth, long-term professional knowledge in a field of specialization. They perform detailed studies and analyses of specific domains (such as improvised explosive devices, surface to air missiles, Islamic culture). They are on call to advise the knowledge manager, combat information specialist, or users as needed. They may come from any sector including university professors, national laboratory scientists and engineers, the intelligence community, and military specialists. An essential enabling service will be the maintenance of a database of experts that can be semi-automatically generated using commercial tools (e.g., Tacit.com, AskMe.com).

Enabling These Roles

Several existing technologies can support each of these roles. These can include wikis, blogs, and collaboration tools. Also key to this approach is defining and staffing new military occupational specialty. Some service activity has already anticipated this need. These new positions help move data laterally across the enterprise activities helping what previously had been stovepiped, inaccessible data.

Imperatives for Enhanced Command and Control

Today, commanders take the command and control of functional areas of combat capability as a given. In terms of combat information, they manage their C2 staff to make sure they get the best information in the right form at the right time. To fully realize the potential of NCO, commanders need to take control of their information and the associated infrastructure (the CIC). This ultimately involves two major elements. First, all commanders clearly recognize that this is one of the critical leadership tasks. Second, the commander will need the staff,

tools, and processes to allow him to get the best situational awareness possible from the CIC.

As much as a fully capable information system available throughout a mission is needed, adversaries are well aware of U.S. dependence on that capability, and they have or may develop capabilities that will allow them to disrupt the CIC in a variety of ways. U.S. actions may also disrupt the capability. The commander must be able to maintain current situational awareness of the CIC and translate the current status to mission capability. The commander must also be aware of enemy efforts to disrupt operations, so that an attack can be countered and a response anticipated to any battle damage of the capability.

As the commander and his/her staff develop mission plans, contingency plans are necessary to plan for degraded operations. The degradation could be in a variety of areas, such as bandwidth, availability, latency, corrupt data, coverage, or protection. Sometimes the result may be an opportunity to operate differently motivated by a change in the situation.

The CIC offers both a challenge and an opportunity. The challenge is stated above. The opportunity is to take a giant step forward by integrating additional Combat Information Capability into the overall command and control function. Commanders need to be able to command and control critical information. This will tend to bring together both kinetic and non-kinetic attack elements into a unified system and, as a step along the way, provide a unified approach to the world of the cyber C2, which historically has been stovepiped and treated in very separate systems. The classic legacy ground battalion/task force tactical operations center with multiple, non-integrated wax pencil map boards is an example of stovepiping by physically co-located staff elements. This unification of C2 processes will allow commanders to have a tool set that supports managing cyber actions and will also allow management of the CIC to support other attack actions.

Specifically, an intellectual foundation is essential for developing future combat information concepts, educating commanders on the art of combat information dominance, and directing commanders to develop concepts of operation and contingency plans for operating with degraded networks.

In order to make this a reality, each service will need to organize, train, and equip cyber capable forces. Training must include network operation and the information management functions that have been discussed. New tools and processes need to be developed for combat information specialists and knowledge managers. These personnel will need to be trained on their tools and the procedures. This training will need to extend to virtual and field exercises such as mission rehearsal exercises, where the command and control of the CIC is exercised along with other joint war fighting capabilities.

Finally, information management staff expertise should be leveraged to doctrinally evolve a combat information planning annex. Similar to other planning annexes such as logistics, the mission plans will address all of the issues with deploying, operating, and defending a CIC in support of operational mission.

Intelligence, Surveillance, and Reconnaissance— an Essential Part of the Combat Information Capability

The war fighter is dependent on ISR sensors for most dynamic combat information. While some part of sensor data is usable only when analyzed, much reconnaissance data requires immediate access because of the time-critical nature of combat operations. Thus, delayed or denied access to ISR information has a significant impact on combat operation effectiveness. Currently, combat information needs compete with national intelligence needs for space asset coverage. The uncertainty of satellite coverage causes operational commanders to rely more on theater controlled assets to ensure coverage, usually to the detriment of lower priority requirements. The lack of knowledge of planned national ISR capability limits integration into the operations tempo and sub-optimizes a limited resource.

Thus, the department needs to recognize the value of treating all space-based airborne (manned and unmanned) systems, and ground and maritime sensors as elements of a single system. Ground combat units are acquiring hundreds of unmanned aerial vehicles with improving sensors. Ground sensors are becoming more effective. All these systems can be more valuable when the data is integrated with other sensor data. The key is to network-enable all ISR data and metadata to ensure timely availability to the war fighter. This capability, when fully implemented, will reduce lead times for dynamic tasking of sensors, thereby greatly reducing the time to respond to time critical targets.

Combat Information Capability needs to be created and resourced across the department, since all military commanders must undertake new ways to execute command and control of their combat information resources and capabilities. In order to maintain oversight, these new capabilities must be monitored by creating a Defense Readiness Review System category for CIC readiness.

To enable the commander to take full advantage of this CIC, Joint Forces Command (JFCOM) needs to develop training programs to prepare commanders to effectively command and control this capability.

A CIC must contain the following capabilities:

- execution elements of a combat information support staff: combat information specialists, knowledge managers, and subject matter experts
- robust combat information management training and education and the capabilities to support such activity
- proper tools and tactics, techniques, and procedures for commanding this new capability.

The CIC must deliver dynamic, integrated ISR capabilities, which will provide operational commanders with visibility of the tasking of sensors and then allow the commanders to effectively plan theater assets.

Recommendation: Create and Resource a CIC

The Deputy Secretary of Defense shall direct:

- JFCOM to establish a training program to prepare commanders to execute command and control of their Combat Information Capabilities.
- The services to create and resource combat information positions, to include combat information support staff, combat information specialists, as well as knowledge managers and identification of subject matter experts. Also, commanders at the three- and four-star level need to be provided combat information integration officers on their personal staffs.
- U.S. Strategic Command (STRATCOM), Under Secretary of Defense for Intelligence, and ASD (NII) to deliver dynamic, integrated ISR capabilities that enable operational commanders to have visibility into national sensor tasking plans, including reducing lead times for dynamic tasking of assets.

Robust Information Management

The GIG is the information technology base (transport, storage, security) underlying a global military information service. Serious attention is required to the “information” aspects, in addition to the “information technology” aspects. However, the Clinger-Cohen Act has carefully defined the “CIO” role, emphasizing—almost exclusively—the information technology portion of the topic. The definition and expansion of this position is required to include managing information content, quality, timeliness, focus, currency, pedigree, relevance, accuracy, and completeness. This new definition will recognize the evolving role of the “CIO” as the earlier, more hardware- and software-oriented definition focused more on assuring interoperability, which is clearly an accepted principle in the evolving information technology and information management world.

Current DOD CIO responsibilities and functions as outlined in DOD Directive 5114.1 (May 2, 2005) are primarily focused on information technology management issues rather than on information content management issues. For example, the DOD CIO responsibilities include:

- evaluating the performance of information technology programs
- reviewing the DOD budget request for information technology
- developing and maintaining the DOD information assurance program
- ensuring the interoperability of information technology systems
- maximizing value and assessing the risk of DOD information technology acquisitions
- prescribing information management policies
- maintaining a DOD Records Management Program
- overseeing development and integration of the GIG
- increasing use of commercial information technology solutions
- ensuring compliance with information technology standards to enable interoperability

While essential to the effective operation of the department, a concomitant set of responsibilities is necessary to oversee the management of information.

Recommendation: Focus on Information

The Chief Information Officer shall expand the responsibilities of all CIO organizations throughout the DOD combatant commands, services, and agencies to:

- establish means and processes to review and assess accuracy, credibility, pedigree, and currency of posted information
- champion policies for information quality, access, and sharing
- implement and distribute incentives for information sharing

- create positions and manage the implementation of the combat information specialists, knowledge managers, and subject matter experts
- identify opportunities for new services in support of user needs.

Chapter 3. Information Dissemination and Management

The Technology Context

Technology advances in the last half of the 20th century fundamentally altered concepts of how people interact with each other, what functions machines can perform, and how the increasing availability of information can reshape day-to-day activities. The Defense Department has embarked on a complex, multi-year transformation to exploit these new concepts for the national security advantage of the United States.

Perhaps the dominant change in this period was the arrival of the Internet. Conceived as a result of Advanced Research Project Agency initiatives in the 1960s, the Internet provided extraordinary opportunities for innovation and led to the creation of vigorous private-sector initiatives to capitalize on its potential. A few characteristics of the Internet—notably its simple standards, lack of a central authority, and public nature—made it the inspiration for much of the technical innovation in the world today. The Internet, with higher level standards that have more recently emerged, is the model for the future Defense Department information environment.

The Internet model has several qualities that align with DOD needs:

- The simple data transport standards enable the interconnection of diverse devices (computers, phones, radios, and televisions, for example). These interconnections have proven to be robust and scalable. Millions of devices can participate together in networks.
- Higher level standards enable information sharing among people and machines. Electronic mail, electronic maps, imagery, and video are common elements of day-to-day life.

- Commercial innovation is bringing new capabilities to market at a rapid pace—a pace unachievable by traditional government processes.
- The ability to rapidly share information and knowledge offers the promise of more productivity. In the case of the defense mission, there is the promise of making U.S. forces faster, smarter, and more lethal than any enemy, through information support to decision-making and execution.

The Internet model also has several drawbacks:

- The Internet model poses challenges for information assurance. In particular, the desire to isolate systems to protect them makes them ineffective for the purposes of sharing information and knowledge.
- The global availability of the commercial Internet means that others, including enemies of the United States, can take advantage of the Internet model without large infrastructure investments in communications and software. The historic advantage U.S. forces have had in these areas is being minimized.
- The pace of innovation has led to shortened product life cycles, implying continual investment to avoid obsolescence.
- The dependence on software, which may have undocumented and undesirable features, has increased.
- The ability to create or modify information environments has not kept pace with rapidly changing requirements and national priorities.
- Management concepts for programs and capabilities work best when applied “vertically;” that is, when each program controls its interfaces and performance criteria to be independent of all others. But to take advantage of the Internet model, capabilities must be implemented “horizontally;” that is, when each program shares its capabilities and data with others and is dependent on them.

The following explores an approach to bring the advantages of the Internet model to the Defense Department while mitigating the disadvantages. Changes to the department's processes for enterprise architecture, technology acquisition, and information management are required. Several recommendations are made to align ongoing programs of record, and further recommendations are made to help maintain the alignment for the future through governance and system engineering processes.

Building the Enabling Capabilities

The foregoing section described the opportunities, along with some cautions and risks represented by the rapid advance of commercial information technology in general and the Internet revolution in particular. The DOD, under the banner of the GIG, is undertaking a set of initiatives—and making substantial program investments—to seize these opportunities, mitigate their risks, and ultimately deliver an enterprise-wide information infrastructure to enable network-centric operations. The delineation of a capability-driven architecture, the execution of an enterprise-level system engineering activity, and the maturing of the new portfolio management process are key elements of the DOD strategy for achieving NCO capability objectives.

This section both describes and assesses the GIG architecture, system engineering, and portfolio management processes and products as understood by the task force, based on presentations from and discussions with government personnel.

The key questions are:

- Whether the architecture provides realizable direction toward fielding NCO-enabling capabilities.
- Whether there is a robust system engineering process in place to translate the architecture into actionable program guidance, and for informing potentially difficult cross-program, cross-organization decisions, as needed, to achieve “horizontal” capabilities.

- Whether the portfolio management process can be informed by system engineering and matured to maximize enterprise capabilities, not just to address the inevitable programmatic issues.

Architecture

Fundamentals

At one level, a basic set of architectural goals can be expressed in terms of building an “Internet-like,” layered information infrastructure which:

- provides ubiquitous networking among information providers and users
- makes information readily accessible, discoverable, and “understandable” across the network
- enables
 - information sharing across the enterprise
 - the development and sharing of a rich set of value-added information services and applications
- assures the security, integrity, and availability of the network and its information by:
 - eliminating bandwidth and computational constraints to the maximum extent possible
 - adopting or adapting commercial products and technology whenever possible while
 - recognizing and responding to uniquely demanding DOD and intelligence community considerations, especially information assurance.

Such a broad formulation of goals, though useful, does not provide a complete basis for guiding and assessing programs and initiatives, or for making decisions. Addressing this issue, the ASD (NII) strategy has been to establish and promulgate—and adopt for “regulatory” purposes—a relatively short list of fundamental architectural principles

viewed as crucial to the building of NCO-enabling capabilities. These principles generally take the form of “design tenets” or “information handling paradigms.”

Design Tenets

1. **Internet Protocol (IP) adoption as the “convergence layer.”** The adoption of the IP commercial standard not only provides for interoperability among heterogeneous systems and devices (currently known and unknown), but also offers the transformational capability to flexibly handle all types of information (such as video, voice, and data) as “converged” streams of packets. The transition to IP-based packet routing/switching and away from dedicated circuits is central to the information handling agility, level of interoperability, and scalability envisioned for the GIG.
2. **“Infinite” bandwidth core/backbone.** This tenet calls for a “core” network, within the larger overall enterprise, which effectively eliminates bandwidth as a constraint within that “core.” Its realization involves the exploitation of optical transmission links in a way that will be elaborated below. The resulting “essentially infinite” bandwidth largely addresses a legitimate concern about adoption of IP—the need to over-provision to assure quality of service.
3. **End-to-end encryption across the core/backbone (“black core”).**
The concept of end-to-end encryption is a cornerstone of the architecture in terms of information assurance. Particular emphasis is placed on maintaining the “all black” flow as information transits the core network, understanding that “red” gateways may be required at the interface between the core and users/systems that lie beyond the “edge” of this core (particularly tactical users who may not be equipped with information assurance devices that “extend” the core).
4. **Data-centric implementation.** The separation of the data from applications and its labeling/tagging enable the capability to have multiple users and/or applications operating on the

same information at the same time, dramatically increasing a user's ability to satisfy his/her own needs and allowing the concurrent development and execution of value-added applications. This design tenet precludes "burying" data within a particular user application and relates closely to the "post-in-parallel" paradigm discussed below.

Information Handling Paradigms

1. **Post data in parallel (as information is created and/or received in "raw" form).** This approach calls for posting data—labeled/tagged as above—before user/application filtering occurs. The intent is to preserve the "raw" data for value-added use by all/any users with appropriate access, including for purposes that cannot be foreseen. This is fundamental to the notion of information sharing, starting at the source. It also enables innovation and unplanned exploitation among users with appropriate access.
2. **User-driven information sharing.** With the foundation provided by data that has been posted and labeled/tagged and is "discoverable"—and with appropriate protection mechanisms—users have the capability to satisfy their own needs for information and to broadly share with others. The potential transformational notion of "smart pull" is facilitated in addition to the paradigms of "smart push" and "publish and subscribe." Sharing is facilitated by establishing a common data dictionary within defined communities of interest.
3. **Need to share vice need to know.** This principle, using a vocabulary that has strongly emerged since 9/11, addresses information sharing challenges when faced with legitimate (though sometimes abused) obstacles in terms of security, privacy, competing mission needs (such as protecting chain of evidence), constraints with respect to U.S. versus. foreign entities. It implies sometimes difficult tradeoffs and the implementation of assurance mechanisms that are not now in place, such as dynamic allocation of access (based on situation or roles of individuals, for example).

4. **Collaboration at all levels.** This paradigm, like “need to share vice need to know,” can be viewed as a special case of information sharing. It is singled out as being of particular operational importance and as demanding particular capabilities from the system. For instance, it implies the provision of common or at least interoperable information services spanning video, voice, and data and operating both in “essentially infinite” and “disadvantaged” bandwidth situations.
5. **Reach-back for critical information and combat operations support.** This principle provides for reach-back, from the theater of operation, to the continental United States (CONUS) or sanctuary locations with substantial information support resources (data, exploitation tools, expertise). This imperative is driven heavily by the priority on leveraging the ever-increasing quality and quantity of ISR information—raw and exploited—that offers critical support to the war fighter.

Note that the fundamental design tenets of “infinite bandwidth” and full end-to-end encryption apply to the core only, not to the networks/systems beyond the core. This is a reflection of realities as one moves into the tactical domain (e.g., disadvantaged users from a communications standpoint). Extending these attributes as far down toward the individual combatant and weapon platform is, however, a priority objective. As will be elaborated below, selective extensions of wideband communications and of the “black core” into the tactical world are offered by major transport programs-of-record—terminals for mobile users with embedded devices supporting IP level end-to-end encryption.

Information Management Architecture

Figure 8 illustrates the information management architecture, including layered elements that ride on top of transport, such as data, enterprise services, community of interest services, and applications. The enterprise services consist of four product lines:

1. Service-oriented architecture framework
2. Content discovery and delivery
3. Collaboration
4. Defense online portal

Information assurance and network operations cut across these levels. Communities of interest leverage these services and subgroups of them are organized into capability portfolios (such as command and control, ISR, joint logistics, and joint network-centric operations).

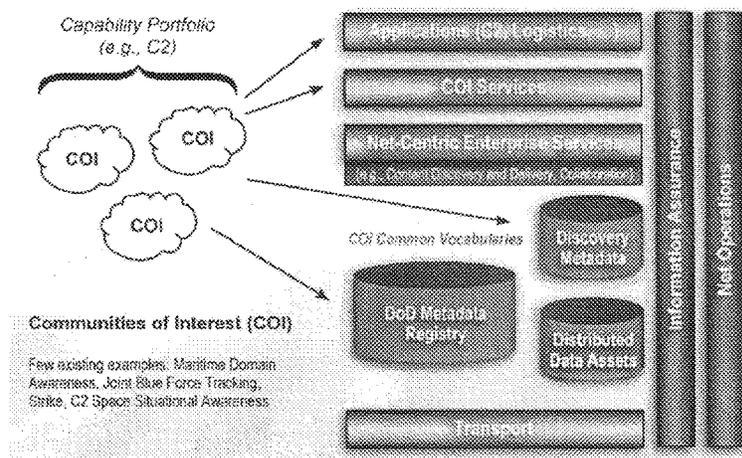


Figure 8. Information Management Architecture

A key concept of net-centricity is to support the “unanticipated user.” Accordingly, security services include strong authentication and authorization services consistently applied across the GIG. These services provide a basis for establishing trust relationships across stovepiped security enclaves. Individual users are validated through certificates, described by attributes about roles, provided visibility to information described by sharing policies, and permitted information access based on policy decision enforcement.

Net-Centric Data Strategy

Net-centric information architecture concepts enable an unprecedented volume of data in a multitude of formats to be shared enterprise-wide. The challenge is to make this data accessible, discoverable, and understandable to every appropriate DOD user. The complexity of the DOD environment introduces challenges—scale, stress, security, range of war fighting/business areas, and multiple lines of authority. The data strategy must support this range of data sources, functions, and environment, enabling the exchange of information between producers and consumers.

The key attributes of the DOD network-centric data strategy are:

- ensuring data are visible, available, and usable when needed and where needed to accelerate decision-making
- “tagging” all data (intelligence, non-intelligence, raw, and processed) with metadata to enable data discovery (by users and machines)
- posting all data to shared spaces to provide access to all users except when limited by security, policy, or regulations
- advancing the department from defining interoperability through point-to-point interfaces to enabling the “many-to-many” exchanges typical of a net-centric data environment

The strategy also introduces management of data within communities of interest rather than standardizing data elements across the department. The strategy separates data from application encouraging interoperability and access, extensibility, and more robustness access control.

Communities of Interest

A community of interest operates in DOD as a collaborative group of people that must exchange information in pursuit of shared goals, interests, missions, or business processes. Communities of interest provide an appropriate focus of net-centric related efforts—to agree on standard community vocabularies, to expose data for discovery and

sharing, and to present common user communities to facilitate providing Net-centric Enterprise Services (NCES) web service capabilities.

The DOD CIO has been active in forming an initial set of communities of interest, including Joint Blue Force Tracking, Strike, Maritime Domain Awareness, and Command and Control Space Situational Awareness. To establish information sharing among its members, a community of interest must:

- Decide what it will specifically accomplish, and the supporting information products that will be required.
- Establish an information model for collaboration, begin to build a common vocabulary, and standardize data. This requires establishing a community of interest data model and framework, including a common taxonomy, vocabulary, and schema. The resultant metadata standards become part of the DOD Metadata Registry.
- Determine what community of interest information sharing capabilities are needed and how the NCES must support it. The NCES services include enterprise web services such as directory, discovery, and security services. Some information sharing capabilities may be unique to the community of interest and require specific services. For example, a user-determined operational picture is enabled by NCES where each community of interest user can personally subscribe and configure information to their particular needs.

Recommendation: Information Management

DOD process owners (Chairman Joint Chiefs of Staff, USD [AT&L], Program Analysis and Evaluation, CIO, Comptroller) shall:

- encourage creation of an information marketplace
- develop resource incentives for making data visible and delivering value-added services
- promote risk-managed information sharing
- deliver value-added services that assess quality of information

The Deputy Secretary of Defense shall ensure:

- DOD components accelerate formation of communities of interest, both top-down and bottom-up (the latter encouraging spontaneity of organization).
- Mission area leads aggregate communities of interest into capability portfolios to rationalize capability portfolio vocabularies and harmonize community of interest services and value-added services.
- USD (AT&L) direct Milestone Decision Authorities to reflect community-of-interest-related capability portfolio goals in direction to program element offices and program managers.
- DOD CIO and designated communities of interest leads co-chair appropriate information technology acquisition boards.

Application Acquisition

While core enterprise services need to be standardized and relatively enduring, the application level demands much more flexibility, rapidity of deployment, and diversity to support user innovation in the face of changing needs, particularly at the “edge.” While there are pockets of such application development, the practice is not widespread in DOD. Programs such as Net-Enabled Command and Control (NECC) are intending the rapid, incremental delivery of application capability. However, the initiation of the program was lengthy, roughly five years from the initial identification of need to the first delivery of capability. Approximately half that time was spent on developing the documentation (of several hundred pages) that specified the needed capabilities. Such a process is not responsive to the immediate and changing needs of the users in the Combatant Commands.

Accordingly, process owners need to revise the Joint Capabilities Integration and Development System (JCIDS) and acquisition system policies to encourage rapid, flexible delivery of application capability increments. Particular steps that should be taken include:

- Change JCIDS focus from detailed specifications to key, high-level capability needs. Such needs should be decided upon relatively quickly and not subjected to a lengthy staffing process.
- Streamline the acquisition resourcing process to allow rapid initiation of development efforts. One possible approach is to allocate funds to a general account without detailed program specification, and then assign funds from this account as specific development efforts are approved.
- Foster innovation by drawing on a diverse set of developers, with a particular emphasis on those from the commercial sector. The philosophy is to maximize capability delivery by allowing any source to provide value-added application services without reliance on a large program structure or detailed capability needs specification.
- Apply the streamlined processes to deliver capabilities in spirals. This entails delivering initial capabilities to operational users prior to defining the entire suite of desired capabilities, capturing feedback from user experience with these (and subsequently delivered) capabilities in operations or exercises, and allowing change of capability development plans in response to this feedback.
- Foster informal development of limited capabilities outside the JCIDS process (even if streamlined as noted above) to get “good ideas” into the hands of users as soon as possible. Developers would work in close collaboration with operational users who test the application capabilities in experiments and exercises. If the delivered capabilities prove worthwhile, then more formal development would be applied if necessary; if the capabilities did not prove worthwhile, the development would be terminated.

Recommendation: Streamline Information Technology Acquisition System

Chairman, Joint Chiefs of Staff and USD (AT&L), revise JCIDS and Acquisition System policies to encourage rapid information technology procurement:

- Significantly reengineer JCIDS for information technology away from detailed specifications to key, high-level capability needs.
- Apply the streamlined JCIDS process to deliver capabilities in spirals. Also focus on “buy and dispose” concepts from commodity type acquisitions (hand-held communication devices, for example).
- Recognize and exploit opportunity to purchase information technology and services as a commodity where practical (routers, switches, blade servers, identity management services).

Research and Development

While human skill and expertise will be the single most important factors contributing to the success of combat information management in network-centric operations, technology that supports that expertise promises significant performance enhancements. Indeed, knowledge managers in commercial enterprises are armed with an array of technical tools for organizing, analyzing, storing, and sharing information. Below is a discussion of the need for similar tools to support the combat information specialist—note that some tools employed by industry may be adopted wholesale; however, others will need to be adapted and yet others developed to meet the unique needs of combat information support. As suggested in figure 9, information management technologies can enhance combat decisions by automatically processing information (extraction, summarization, correlation); generating user tailored and/or contextually situated presentations, supporting a range of cognitive tasks (focus of attention, pattern detection, and comparison, for example); and decision support (such as applying knowledge and experience to generate, assess, and select among alternative courses of action).

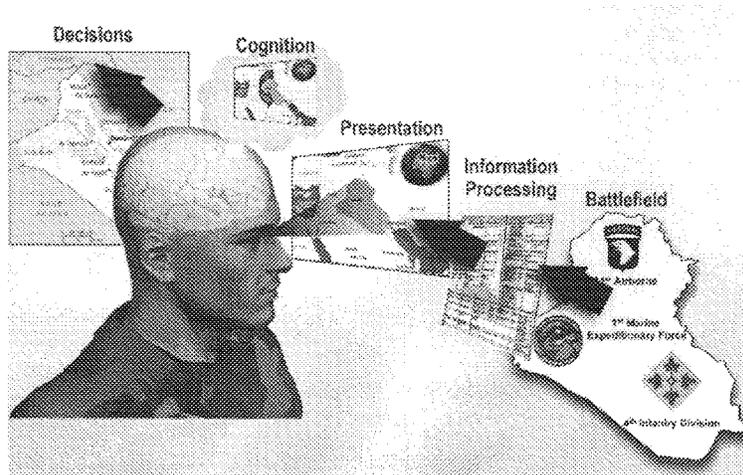


Figure 9. Information Management to Enhance Combat Decisions

Information Discovery

In each of these areas, research promises advances that can transform operations. For example, in the area of information discovery, intelligent analysis of content promises several benefits. Automated metadata tagging of documents can be used to annotate massive collections of reports and captured documents to provide enhanced search and discovery. Operations will require advances beyond the state of the art to include 95 percent accurate entity tagging (that is, people, organizations, and locations) and 80 percent accurate event extraction in English and foreign language text (current state of the art is around 90 and 50 percent, respectively, for text).⁶ Soldiers also require automated voice transcription of after-action reports to increase the timeliness and coverage of reporting. Forces also need automated content extraction from multimedia, such as unmanned aerial vehicles or surveillance video, as well as audio intercepts and reports. Operators also require tools for semi-automated assessment of quality and

6. See: trec.nist.gov.

relevance of information. Locating quality information rapidly on a dynamic network that might be degraded under attack coupled with the need to provide more fine-grained (subdocument) access control, suggests that services such as Uniform Resource Names can help resolve information references and provide more reliable and fault tolerant access to information.

Information Understanding

In addition to more effective discovery of information, advances are needed to enhance cognition and information understanding in the context of missions. Increased information understanding can lead to a 50 percent improvement in situational awareness and a two times speed up in understanding. Advanced understanding tools are required to automatically associate, cluster, fuse, and summarize information. For example, automated document summarization (SUMMAC⁷) has been shown in science texts to reduce text by 80 percent with no information loss. Understanding the meaning and implications of information are important and will require effective application of knowledge representation and reasoning. For example, ontology management tools (creation, merging, refinement) can be applied to enhance semantic machine-to-machine interoperability.

Tools for information triage (based on relevance, priority, and quality) to counter information overload as well as tools to counter denial and deception will become increasingly important. Finally, operators need context-aware presentations that are sensitive to a variety of environmental factors (location, time, and device) as well as to the psychological, perceptual, cognitive, and social characteristics of the user and groups. Addressing all dimensions of context management (time, location, mission, user role, ongoing dialogue) promises more efficient and effective operations, particularly for (bandwidth, presentation, attention, and memory) disadvantaged users. A key future capability will be to learn users' context, information needs, and preferences through observation. As this technology matures it will

7. http://www-nlpir.nist.gov/related_projects/tipster_summac

allow the staff functions of a combat information specialist, knowledge manager, and subject matter experts to become more fully automated.

Information Sharing

In addition to improved machine understanding, effective information management requires enhanced, machine-facilitated, human-human interaction. Information sharing between the United States and coalition partners can be enhanced with semi-automated dissemination that leverages information bases that are tagged both in terms of discovery metadata (bibliographic, security) as well as content metadata (entities and events in the text). Semi-automated dissemination and tailored information packaging promises to reduce requests for information from the field by over 50 percent (of Joint Intelligence Center Pacific⁸) by dissemination to appropriate classification (sensitive but unclassified, SECRET, TS) and/or release (coalition, nongovernment organization), based on both security and content mark-up. Tools that facilitate knowledge elicitation (such as leveraging but extending beyond DARPA ASSIST to support effective automated debriefing) are needed to support functions such as semi-automated capture, processing, and dissemination of after action-reviews and lessons learned. Finally, enterprise collaboration services (such as presence and awareness) need to provide context-based, mission- and role-tailored discovery, collaboration, and sharing.

Information Marketplace: Warrior Tracking and Behavior Analysis

Enabling the management of and fostering the growth of an information marketplace will require mechanisms to understand user information needs, tools to design information services and control and tailor delivery, and mechanisms to assess the quality of delivered services. Information and information services monitoring will require mechanisms to audit and analyze user information consumption and utilization behaviors. To create richer models of the information

8. http://jicpac.com/web/about_jicpac.html

marketplace understanding will need to go beyond instrumentation of warrior behavior to include:

- surveys
- post-mortems
- more generally, ethnography of information service providers and consumers
- analysis of social drivers (identity and reputation, rewards and incentives)

Recommendation: Information Management Research and Development

Director, Defense Research and Engineering (DDR&E) establish and extend programs for:

- Information discovery
 - auto generation of metadata/auto-tagging
 - tools for assessment of quality of information
 - content extraction from unstructured text/video/audio
 - advanced discovery tools
- Information understanding
 - fusion and association
 - cognition and information understanding in the context of missions
 - knowledge representation and reasoning (ontology)
 - context aware presentation
- Information sharing
 - knowledge capture
 - context-based, mission, role tailored discovery, collaboration, sharing

- collaboration—presence/awareness, tailored
- Semi-automated dissemination
- Net warrior tracking, behavior analysis
 - audit, capture, analysis of use/change
 - surveys, post-mortems, instrumentation, ethnography

System Construct

The basic system construct for implementation of the GIG NCO-enabling architecture is depicted in figure 10 below. This greatly simplified depiction is intended to convey key features of the architecture in “physical” terms. Several programs-of-record, those viewed as delivering particularly key capability “building blocks,” are indicated. Although dealt with in more depth in a subsequent section, these elements are shown here to make this description of the construct more tangible.

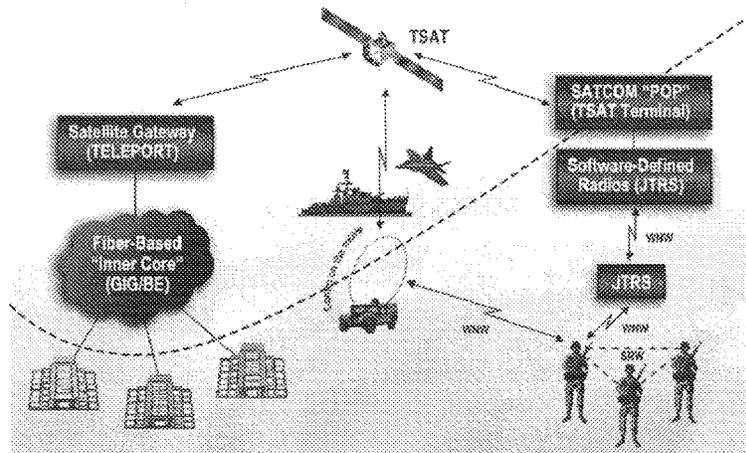


Figure 10. Key Transport

The architectural notions of (1) a core/backbone network providing “infinite” bandwidth and IP level end-to-end encryption among users and providers located in the CONUS or in selected sanctuaries, and (2) interfaces with, and extensions to, tactical level users/platforms (including mobile), were introduced above. More specifically, the NII-delineated architectural construct, as depicted in figure 10, consists of:

- A two-level core/backbone network with the noted “infinite bandwidth” and IP-level end-to end encryption attributes.
 - An “inner core” with meshed, fiber-based connectivity among CONUS and selected sanctuary locations outside CONUS, implemented by the Global Information Grid/Bandwidth Expansion (GIG/BE).
 - An “outer core” that extends from the “inner core” to theater locations via wideband satellite communications and, using Internet terminology, provides a core network “point-of-presence” (POP). The Transformational Satellite Communications System (TSAT) is a key capability to achieve this.
- A set of wireless, line-of-sight-radios/devices beyond the core but (1) interfacing to its “edge,” either directly or through “intermediaries” (e.g., the Army’s Warfighter Information Network—Tactical) and (2) providing IP-based capability along with substantially greater capacity than current tactical radios. The Joint Tactical Radio Systems (JTRS) program is the principal new capability. There are also a variety of legacy upgrades and commercial options being considered in the interim.
- Exploiting the above transport architecture, the conduct of network-centric operations will enable communication:
 - among users and providers who are directly connected to the “inner core” (such as various intelligence nodes and major fixed bases)
 - between users and providers directly connected to the core and those beyond its “edge,” with satellite-based reach-back as a key feature

- among user and provider communities of interest or enclaves that reside beyond the edge

Note that, as depicted, both TSAT and JTRS (or some equivalent) provide critical capability from the viewpoint of the tactical user. TSAT will uniquely provide relatively wide bandwidth connectivity to small, ground-mobile platforms, supporting “command and control on the move;” JTRS is designed to provide both a wideband networking waveform (WNW) for meshed inter-netting among mobile platforms and tactical C2 facilities, with the soldier radio waveform (SRW) providing analogous capability among individual combatants.

Though the communications foundation for NCO is surely a crucial enabler, the delivery of operational capability in terms of “information as a weapon” is found at the upper layers of the architecture. In this regard, two features of the architectural construct stand out:

1. Adoption of a service-oriented architecture, meaning the provision of a common set of software-instantiated middleware services that are accessed from across the enterprise network and enable applications/users to exploit the network and its data (a discovery service or an identity management service, for example).
2. Adoption of a community-of-interest strategy to facilitate mission-driven information sharing, meaning the creation of a collaborative group of information users and providers who organize around a mission (such as maritime domain awareness, space situational awareness) and develop a common vocabulary for machine-to-machine information exchange.

Finally, it can not be over-emphasized that there are serious information assurance challenges that go beyond the implementation of the “black core” and will impact the architecture in ways that are only now emerging. This topic is the subject of a separate chapter.

Observations

As discussed above, architecture fundamentals have been articulated and a basic system construct, a top level system design, has at least been outlined. The bottom line architectural findings are:

1. The architecture, as understood by the task force, is viewed as sound and as constituting positive direction to the department's efforts to field an NCO-enabling information infrastructure.
2. On the other hand, it is not articulated consistently or elaborated substantively in any one place or product. Also, there are crucial interpretational and definitional issues regarding the meaning of the fundamental tenets and paradigms as evidenced in both dialogue with government presenters and within the task force itself. This may well impede "unity of action."
3. More fundamentally, even if the architecture were "perfect," there is the critical job of translating its fundamentals into tangible, actionable program guidance and assuring that the department's set of implementing programs yield coherent "horizontal" enterprise capability.

The concerns identified here are addressed in the following discussion of system engineering.

System Engineering

It can be argued that the department faces an unprecedented system engineering and related governance challenge, given the scale of the enterprise and the need to build inherently "horizontal" capability in the world of "vertical" programs and organizations. Addressing this challenge is a central element of treating the NCO-enabling information system as a critical combat capability or as a "weapon system." This section characterizes the ongoing enterprise system engineering activity and develops a set of recommendations. A later section addresses the governance issue in the context of the "portfolio management" process that has emerged from the Quadrennial Defense Review.

Ongoing Efforts

An “enterprise-level” system engineering activity is needed to:

- translate the architectural fundamentals into tangible program guidance
- analyze and trade among program and design options with a constant focus on overall enterprise functionality and performance
- support cross-program and cross-domain decision-making

A critical objective is to assure coherence among the key programs developing and delivering the essential “building block” capabilities. Synchronization of delivery across programs from a mission capability standpoint, is another objective. Figure 11, below, without even penetrating the detail, illustrates the challenges.

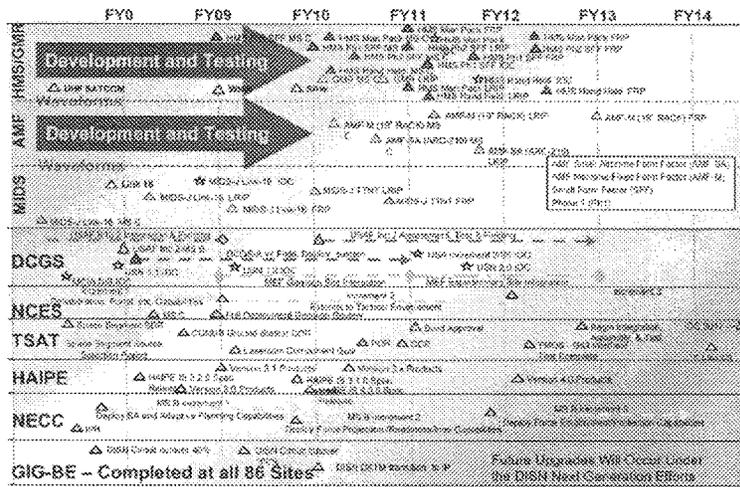


Figure 11. Net-Centric Programs Schedule

The ASD (NII) established an Enterprise-Wide System Engineering (EWSE) office in 2004. The Defense Information Systems Agency (DISA) is assuming increasing responsibility for this function with continuing NII oversight and involvement. The ongoing efforts are struggling with the differences between executing a system engineering process at the enterprise level as opposed to the individual program level. Formalistic specifications, flow-downs to “subsystem” specifications, and work break-down structures, are neither desirable (too constraining) nor practically realizable (scale and complexity). It is noteworthy, in fact, that the larger technical community is only now struggling with the art and science of large scale, complex—read “enterprise”—system engineering. So, the department is breaking new ground in some respects. This fact, along with the obvious “horizontal” versus “vertical” governance and authorities issues, yields the term “unprecedented.”

The NII-led EWSE activity is executed by a core team of government, federally funded research and development center, and contractor personnel, plus “coalition of the willing” (and available) service and agency participants. There is surely good news in terms of (1) serious technical work on critical enterprise-level issues, such as assuring quality-of-service across the network, (2) development of initial guidance products that lay out standards that would assure interoperability and Internet functionality, and (3) at least the beginnings of an analytically-based effort to estimate and bound end-to-end performance from a user standpoint.

Observations

Positives notwithstanding, the task force developed a set of concerns about the current activity:

- The effort attempts to be comprehensive in terms of the scope of mission and functions (such as GIG support of DOD business processes as well as war-fighting). This is understandable and, in fact, appropriate, given the NII/CIO charter. However, comprehensiveness does not allow clear focus on the delivery of combat information capability.
- The technical work exhibits a tendency to over-engineer and over-optimize across a broad range of issues without clear prioritization based on mission functionality and performance

impact. For instance, the analysis of end-to-end latency versus different quality of service and precedence schemes is important, but only if the latency differences matter from an operational standpoint.

- The strategy for influencing programs seems to rely on relatively detailed, prescriptive guidance documents (network-centric implementation documents) with enforcement through control and compliance processes. This is different from limiting prescription to a few, absolutely crucial elements of guidance, and then actively engaging collaboratively with programs on the longer list of issues and trades that need attention from an enterprise viewpoint. (The involvement of “coalition of the willing” service and agency program participants, noted above, is inherently spotty and does not constitute adequate engagement from the viewpoint taken here.)
- Despite good intentions and plans, it appears that the effort devoted to analysis, simulation, and test-bedding (at least to date) has been extremely limited. Not only does the serious execution of such work constitute good engineering practice, but such work is particularly crucial at the enterprise level. At this level, scale and complexity defy confident predictions based on appropriate engineering analysis of design integrity and end-to-end performance.
- The efforts to date have focused almost exclusively on “transport layer” issues and guidance. This too, is understandable due to “essentially infinite” bandwidth as a key foundation tenet, large, complex, and costly programs-of-record needing front-end guidance (especially TSAT). But, as per a major theme of this study, “it’s all about the information” when targeting combat value. It is understood that the need to re-focus priorities toward the upper layers (enterprise services, data, and applications) is being reflected in current EWSE planning.

Capability Portfolio Management as a Key Element of Governance

DOD needs to manage information technology investments as capability portfolios to efficiently and effectively deliver capabilities to the war fighter, and maximize return on investment to the enterprise. Portfolio management goals include:

- Transitioning from program-by-program investment management to end-to-end portfolio management that ensures portfolio recommendations are reflected in the JCIDS, the defense acquisition system, and the Planning, Programming, Budgeting, and Execution System processes and decisions.
- Expediting the capability to advance network-centric operations by collectively assessing net-centric transformation and synchronizing capability delivery across the department's infrastructure.
- Minimizing programmatic, technical, and operational risks by choosing the best mix of investments within the portfolio.
- Leveraging opportunities to collaborate with other portfolios to advance mission effectiveness, identify and manage interdependencies, and foster net-centricity.
- Expediting convergence toward net-centric capabilities; reducing unnecessary capability duplication; capitalizing on "best of breed" information technology solutions already fielded; and improving efficiency, cost-effectiveness, awareness, and access to capabilities and services across the enterprise.

A minimal governance regime, led by the DOD CIO and informed by GIG architecture principles and systems engineering, is required to make and oversee execution of capability portfolio recommendations. The governance regime must drive the department-wide information technology capability by aligning similar initiatives and coordinating investments, overseeing the development and deployment of the department's information technology infrastructure, and rigorously enforcing policy and decisions with attention to execution and accountability.

As recommended above, system engineering should focus on war fighting capabilities, and concentrate on the key specifications for the GIG core and the interfaces to the tactical enclaves at the edge. Systems engineering informs the capability portfolio management process by describing the technical issues and trade-offs, and recommending courses of action.

To resource the transition to a net-centric environment, opportunities to reduce operations and maintenance expense must be identified. Operations and maintenance costs to support disparate, non-compatible information technology systems grow significantly over time and are hidden in the undefined operations and maintenance cost elements of the services. This means finite resources are being ever more consumed by non-centric systems. Capability portfolio management and the governance regime must generate sufficient savings to resource the needed transport, services, and information assurance capabilities.

Technical Workforce

The challenge of developing enterprise-wide information management (and more broadly, GIG) capabilities is great, given the complexity and scale of the deployed capabilities. This requires a highly competent technical workforce on the part of DOD. Over the years, the technical depth of DOD's workforce has decreased. The problem is further compounded by the facts that skills in new technical areas are needed for information management (and, more generally GIG) development and more rapid development is required. Advanced information technology and information management skills, as well as development velocity, are much more in evidence in the commercial sector than in the DOD.

Recommendations: Governance

USD (AT&L) and DOD CIO establish effective net-centric governance:

- aggressively implement comprehensive capability portfolio management (such as requirements, resources, acquisition, testing, operations, and sustainment)

- re-orient enterprise wide systems analysis and engineering:
 - to focus on war fighter capabilities and performance metric development
 - to concentrate on informing the capability portfolio management process
 - on key specifications for the core and interfaces to the edge
 - to establish and assess key performance versus assurance trades

The Under Secretary of Defense for Personnel & Readiness develop a strategy to establish an adequate technical workforce to deliver net-centric capabilities. Particular objectives to be accomplished by this strategy should include:

- Establish a small cadre of world-class experts within government to develop the net-centric technical vision and implementation plans. Attracting such individuals from the commercial sector for career employment in DOD would be difficult. However, rotating individuals in from that sector (such as for three years in a Defense Advanced Research Projects Agency (DARPA)-like model) could prove feasible because the opportunity to work the unprecedented technical challenges confronting DOD without permanently giving up their commercial employment could be attractive.
- Ensure DISA has the necessary staff and expertise to execute its increasing role in developing and operating net-centric capabilities. Since DISA reports to the ASD (NII), it should play a lead role in determining and advocating the need for the staff required at DISA for its mission.
- Ensure adequate systems analysis and engineering expertise to determine design trades and conduct technical analyses. Significant systems analysis and engineering expertise exists across the DOD components. DOD leadership (particularly the USD [AT&L] and the DOD CIO) should work to bring this expertise to bear in as collaborative a manner as possible to address enterprise needs affecting information management

(and the GIG as a whole), and augment this workforce with new staff as necessary.

Providing an adequate number of technical operators and training for those personnel for running deployed capabilities. The services and agencies would be responsible for providing personnel and their training to support the needs of the combatant commands for the operation of both networks and services.

Current Key Programs

In reviewing the important architecture principles and construct for the future DOD information management system, the task force examined those current programs-of-record that form the principal basis for building and realizing the architecture. These programs are described as follows:

- **Global Information Grid/Bandwidth Expansion.** The GIG/BE program provides an extensive fiber-based IP network infrastructure. It is being acquired by DOD, ultimately with plans to have nearly 100 nodes operational world wide. This terrestrial infrastructure will support extremely high (“infinite”) bandwidth, and forms the fundamental “inner core” backbone for the GIG transport layer. As of August 2006, this program had completed 86 nodes worldwide, and initial operational testing and evaluation is ongoing.
- **Transformational Satellite Communications System.** A large scale DOD program to extend the GIG/BE to theater POP and to provide significantly enhanced intra-theater communications. The major segments include:
 - Space. A five satellite constellation with each satellite cross-linked with laser communications as well as optical links for transfer of IS data collected by airborne platforms.
 - Mission operations. The TSAT Mission Operations System (TMOS).

- **Terminals.** A family of terminals for fixed ground and mobile platform use, including small dish radio frequency terminals supporting command and control on-the-move.

The program is currently following a block acquisition strategy, with Block 1 including the first two satellites and Block 2 the remaining three satellites. The first satellite is scheduled for launch in 2014, and Block 1 will have limited laser as well as radio frequency communications. The Block 2 satellites will have the full optical and radio frequency capability, with those launches starting with satellite #3 currently scheduled for 2017. Key technical issues being addressed currently that are vital to system realization include timing and tracking of the in-satellite processing router as well as acquisition and angular pointing technical challenges for the laser communications system.

- **Joint Tactical Radio Systems.** JTRS is a family of radio systems based upon software waveforms that, when implemented, will extend the TSAT point of presence to the tactical (vehicle) and individual combatant, in effect pushing the edge of the network core outward toward the individual warfighter. JTRS radios will also provide for meshed, IP-based inter-netting among enclaves of tactical users. The key waveforms to enable this extension and associated *ad hoc* tactical networking were uniquely developed to support tactical operations. These unique waveforms are the wideband network waveform and the soldier radio waveform. In addition, the JTRS capability has an objective to include numerous legacy waveforms, and depending on the JTRS variant, would be interoperable with potentially up to 32 different waveform types. (A decision was made to eliminate cellular waveforms from the JTRS program, thus not enabling COTS cellular handsets interoperability with JTRS.) Due to schedule issues with the JTRS program, the Army and the Air Force have been aggressively pursuing interim approaches to enable the soldier radio and wideband network waveforms to be fielded immediately, particularly within SINGARS/EPLARS.

- **Network-Centric Enterprise Services (NCES).** NCES is a set of basic common software services to be operated on the unencrypted (“red”) side across the GIG enterprise. These services, when fully operational, will enable information providers to post or share information, to discover other information resources, and to collaborate dynamically. Core services currently planned include collaboration, service management, storage, application, messaging, user assistance, discovery, security management and information assurance, and mediation. Plans for acquisition include, (i) buying available (mature) commercial products, (ii) adopting services using proven specifications and existing web-service technologies, and (iii) if necessary, creating new services via software development.
- **High Assurance Internet Protocol Encryption.** HAIPE is an acquisition program that provides IP-level traffic protection via end-to-end encryption, routing, and network services. HAIPE can be standalone or embedded in a host platform, and provides the functionality of protecting a node or enclave. The HAIPE program and its resultant products are expected to form a key component of the GIG information assurance architecture. Although the HAIPE program as planned does not encrypt all data (some bypassing occurs such as with signaling and quality of service bits in the data stream), the key payload information is encrypted. The current realization of HAIPE (v. 1.3.5) is already being used within the DOD, with four commercial vendors having demonstrated compliance with the government specification. By mid 2008, it is expected that the compliance standard will be 3.0, a software upgrade that will provide enhancements such as improved bandwidth efficiency, added ability to do remote upgrades, and enhanced discovery and quality of service.

Recommendations: Transport Programs

This task force purposely did not perform an in-depth review of the various applicable DOD programs of record. However, in the process of examining the overall state of progress in developing component

capabilities, the task force did extract the following observations and recommendations:

- The overall vision of moving the department toward its information management vision would be helped if the financial incentives that, in effect, subsidize voice traffic on GIG/BE would be matched with comparable incentives to encourage use of the GIG/BE for data. In addition, existing teleports can be used to extend the core for GIG/BE. The task force also encourages integration of the Distributed Common Ground System Integration Backbone with the GIG program as soon as possible.
- The task force encourages the TSAT program to develop wide field of view optical receivers to mitigate some of the acquisition and pointing issues as well as to augment bandwidth. The TSAT program should also emphasize inter-theater communications in its design and development.
- Due to the importance of achieving the key JTRS functionality and war fighter capability as rapidly as possible, the task force recommends that the JTRS program prioritize deploying the wideband network and soldier radio waveforms to key weapons and sensor links.

Recommendations: NCES and HAIPE

The task force is very concerned about the DOD's dependency on two critical programs in achieving its network-centric information management vision: NCES and HAIPE. The success of these two programs is required to achieve DOD's net-centric vision. Each program has a number of key issues that need to be resolved and therefore are highlighted separately by the task force.

Net-Centric Enterprise Services

Issue. The NCES development and delivery appear to be highly complex as currently planned by DOD. The acquisition strategy and related governance offer several areas of risk. For example, the task force is concerned about the depth of critical skills required by the

government to effectively perform source selection and subsequent program oversight in this new acquisition approach. A related concern is the complexity of governance where a single overall integrating contractor and individual service providers are all potentially operating under separate service level agreements, offering potentially confusing lines of authority and governance. An additional concern regarding the NCES is their attractiveness as an information assurance target due to their ubiquity across the enterprise and their residing unencrypted outside the black core.

USD (AT&L) and ASD (NII) must address critical Network-Centric Enterprise Services programmatic issues:

- Rapidly attain and sustain pace with commercial capabilities.
- Expand current efforts establishing a collaborative development and testing environment.
- Establish clear lines of authority and responsibility for delivery and operation, ensuring that the NCES and NECC initiatives are synchronized.
- Take special care in the design to include information assurance. NCES is not protected by encryption and, being in the “red,” is a significant target. Attention must be paid to this potential vulnerability.

High Assurance Internet Protocol Encryption

Issue. There remain some difficult unresolved technical issues in the HAIPE program, such as achieving an efficient means of achieving HAIPE-to-HAIPE discovery through the black core. In addition, there remain issues with successful implementation of typical level three network services across the HAIPE functionality (such as quality of service), and, in general, of keeping pace with the state of technology in commercial networks.

USD (AT&L) and ASD (NII) must address critical High Assurance Internet Protocol Encryption programmatic issues:

- Rapidly attain the functionality to support existing and future trusted commercial network services that allow the outward expansion of the black core; and
- Continue research and development (R&D) on IP address discovery and mobile *ad hoc* networking.

Tactical Edge Networks

The architectural and programmatic considerations discussed above apply to all users within the chain of command. Particular attention, however, must be paid to users beyond the core who operate with “tactical edge” networks. These users will typically be mobile and require information management support to maintain situation awareness and to synchronize operations. Much of the information needed by these edge networks will be provided by direct exchanges among them and with immediate higher echelon headquarters, but they will also reach back to the core for some information, as well as send tactically derived information back to the core. Furthermore, much of the necessary information will not be held in some formal database but rather be derived from verbal or message accounts of the tactical environment, although that information should be posted to the core as soon as feasible.

The tactical users typically have more limited capabilities than at higher echelons. Particular factors are:

- the need to operate in a physically stressing environment
- limitations in bandwidth capacity
- restricted size and capability of display devices
- potentially frequent disconnection from the broader network

Attention is being paid to improving tactical communications. However, the particular aspects of information management to support tactical users, while critical for mission success, are a largely neglected subject.

Accordingly, the task force recommends that the services, in conjunction with combatant commanders, tailor information management to support delivery to and from the edge. Particular steps that should be taken include:

- Delivering applications that adapt delivery to tactical user bandwidth capacity and display capability. These applications would involve automatic and manual content and presentation filtering making use, for example, of metadata tagging.
- Implementing content staging to furnish information caching forward providing more timely access to the information.
- Ensuring standards-based tactical interfaces with the core to allow ready access to information in the core, as well as delivery of tactically gathered information back to the core.
- Providing ready means for reengagement of frequently disconnected users (such as services to synchronize data stores).
- Developing concepts of operations and policies for the combat information specialist and knowledge manager that explicitly take into account the needs and limitations of tactical users.
- Ensuring the survivability and reconstitution of the system both in terms of network connections, as well as in terms of information and applications (such as peer-to-peer information sharing and applications).

All these information management improvements should be made along with improved tactical communication networks, preferably through the provision of robust, *ad hoc* meshed tactical networks and peer-to-peer information and application management. For rapidity of deployment and to keep abreast of the latest technology, these tactical networks should leverage commercial technology to the maximum extent feasible.

War Fighters Need Special Combat Information Devices

Providing combat information to the edge will require innovative devices that will be low power, rugged, operate in a variety of light conditions, integrate voice and data communication, and essentially be the single portal to the tactical fighter for combat information, communication, and collaboration. This device needs to recognize the realities of the tactical environment, and thus be simple and intuitive to operate. This portal device could potentially be adapted from commercial technology, as illustrated in figure 12. Cell phones, personal digital assistants, and portable game devices should all be explored as candidates to meet this important operational need.

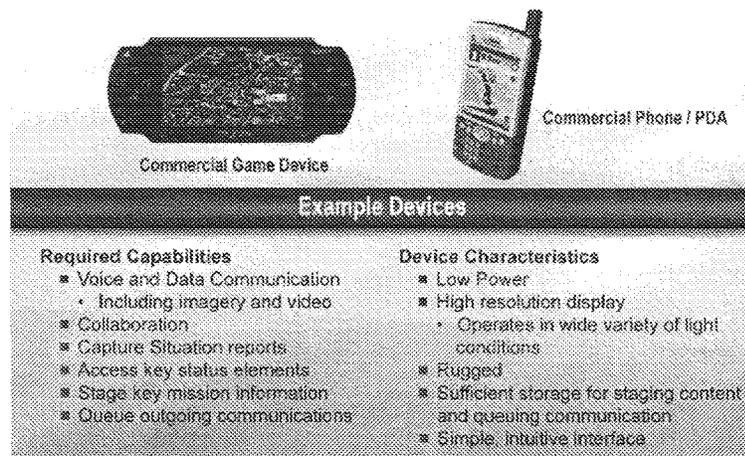


Figure 12. War Fighter's Combat Information Portal

The operational device should provide war fighters the following capabilities:

- voice and data communication with the core mission team as well as other entities, such as a combat information specialist, joint forces, coalition forces, and nongovernment organizations
- collaboration in support of situation awareness, planning, mission rehearsal and execution
- blue force positional information
- situation reports such as SALUTE reports
- access key status elements such as CIC and network status
- stage key mission information locally, as well as queue key communications when the network is down

For this device to be practical, it will need to have the following characteristics:

- low power
- operate in a wide variety of lighting conditions without compromising a combatant's position
- rugged to withstand the rigors of combat
- sufficient storage for staging content and queuing communications

Commercial capability can be easily and economically adapted to meet this requirement. The objective is to have these devices so inexpensive that newer generations of technology can be quickly fielded to maintain the tactical advantage and avoid technical exploitation by an adversary. The use of commercial data and communications devices to form true COTS capability within edge networks must be compatible and interoperable with the last points of presence defined by the backbone core network. These points of presence may be a TSAT, WIN-T or JTRS terminal. Tactical networks must also be capable of forward staging and caching of critical applicable data needed for specific tactical objectives.

Recommendation: Support Tactical User at the Edge of the Core

USD (AT&L) and DOD CIO, ASD (NII):

- Deliver robust, easily formed, meshed tactical networks that leverage commercial technologies.
- Deliver applications that adapt delivery to tactical users' display and bandwidth (exploit information metadata).
- Implement robust content staging to provide information caching forward to enable timely access.
- Ensure standards-based tactical interfaces with core.
- Develop unique and local security strategies.
- Resource information management staff to support tactical users.
- Reintroduce cellular waveform into JTRS.
- Analogous to the approach to the HAIPE initiative, offer incentives to the private sector to implement soldier radio waveform into the core waveform set in the commercial world—encourage the production of future commercial capabilities that meet the department's needs.
- End-user devices (such as Blackberry and Treo) are commodities, and should be acquired using commodity acquisition methods, such as the General Services Administration Schedule.

Chapter 4: Critical Information Assurance Challenges

Network/Information Assurance as a Strategic Issue

Contemporary DOD and related national security net-centric operational environments have serious current and future problems related to maintaining confidentiality, availability and integrity of information. Information assurance is a descendant of information security, an older discipline that worried almost exclusively about keeping secrets—the “confidentiality” of data. The change in nomenclature was made to accentuate the fact that there must be concern not just with the confidentiality of the data but also with its integrity and availability.

Although the nomenclature has changed, too often the emphasis remains on confidentiality. There is reason to argue that in the martial context, with the coming of net-centric operations and the unforgiving dependence on information from afar, there should be much more concern with integrity and availability. One salutary outcome of the persistent storm of attacks on the Internet is that some—the denial of service attacks, and distributed denial of service attacks—have sensitized DOD to the issue of availability.

Consider integrity, the fact that a malicious user may have changed the data, not just randomly, but according to some intelligent design. Two equally bad outcomes: one fails to notice and acts on deliberately misleading information; or, one notices and can no longer have trust in any of the data or, both happen sequentially. The loss of trust either in the ability of the system to deliver any information, or correct information is most insidious. Loss of integrity raises one of the most vexing challenges: how to restore trust in the “network” once you have lost it.

The threats to the networks and related communications, and information technology architectures and components, are neither well

appreciated nor fully understood. In particular, there appears to be a high level of naiveté among network participants about information assurance risks and issues, or even outright hostility to having to deal with information security communities and problems.

Given that the network environment is, and will continue to be, heavily comprised of COTS hardware and software, which are increasingly being developed offshore, reducing the threats to networks will be a complex, relentless, and often frustrating undertaking. Even more significantly, there are important network trends and aspirations in being able to maximize information at the edge of the network with previously disadvantaged users. In effect, the larger the network, the more points of vulnerability to the networks is introduced. Finally, the DOD acquisition system is currently not capable of keeping up with the speed of COTS, nor is there any notion of how to harness the speed of COTS (or to provide incentives for the high speed invention of COTS) to DOD's network and information assurance advantage.

Formalized Risk Management

The nature and character of both future insider and outsider risks to the network may be more pervasive than in any earlier time in DOD history, and DOD must develop strong and formalized "risk management" processes and tools to continually evaluate and define directions for mitigating the threats.

In the case of information systems, cost is determined in the marketplace, as is the case with COTS. When a potential vulnerability is pointed out, there's a tendency to balk at the "exorbitant" cost of hardening that capability—the true cost of information assurance.

Further, there is a myriad of known vulnerabilities and an endless supply of bad actors. Too little insight into their actual motives and capabilities, doctrine, tactics, techniques, procedures, and their "political will" is known. This is especially true with respect to the more-to-be-feared high-end adversary, generally state-sponsored, well-resourced, and highly disciplined—unlikely to mindlessly reveal their true capabilities and intentions. These parameters, quantitative costs, and

values are essential to rational risk management. Presently, DOD does not have a good handle on them.

Threats

As dependence on networked capabilities grows, along with the ability to demonstrate improved military capabilities, adversaries will become increasingly motivated to attack information infrastructures. Dependence is, perhaps, the ultimate asymmetry and it has not escaped notice. There is ample evidence that U.S. adversaries have recognized this potential vulnerability and are aggressively developing doctrine, tactics, and technology to attack this soft underbelly.

Therefore, to leverage the net-centric operational advantages with high confidence, an adversary's capabilities, intentions, and specific targets within the GIG and extended networks must be deeply understood. Insight into an adversary's offense is a necessary but not sufficient condition for performing effective risk management. Equally important is to understand the effectiveness or shortcomings of various defensive tools and approaches in mitigating an adversary's operations.

There are several factors that contribute to the complexity and criticality of balancing the utility of net-centric and consequence of compromise. First, current dependency on information technology infrastructure is extremely high and the dependency of the envisioned net-centric architecture will be significantly greater. This increasing reliance provides an escalating motivation for an adversary to target elements of the architecture. There is growing evidence that many adversaries will recognize this vulnerability as an asymmetric opportunity and will develop strategies, organizations, and associated capabilities to target these systems.

Second, a significant and increasing percentage of the technology used to build these systems is COTS. Even if this technology is acquired from U.S. companies, the provenance of the technology is increasingly foreign. The complexity of both the microelectronic and software components is enormous. Consequently, the challenge of discovering malicious constructs introduced by an adversary through

these life-cycle opportunities is exceedingly difficult. As will be shown, this aspect alone provides considerable benefit to an opponent.

Finally and closely related to the dependency issue, the impact of a defensive failure (confidentiality, integrity, or availability) is enormous and will likely grow to unacceptable levels unless mitigating strategies are discovered and employed. Alternatively, new approaches (war modes and hedging, for example) and architectures can be developed such that the compromise by an adversary will have reduced impact.

With these factors in mind, can these adversarial advantages be sufficiently offset to warrant the desired benefit? This task force concludes that the current state of the defense will be considerably outmatched by a sophisticated, well resourced, and motivated opponent. To more deeply appreciate the basis for this conclusion, a characterization of such an adversary is needed.

A sophisticated and effective intelligence organization, intent on conducting aggressive and modern espionage operations against its opponent's end points, will possess many of the following capabilities and characteristics:

- worldwide presence
- mature operational tradecraft (allows for full and non-alerting integration of case officers, assets, and technology into the target environment)
- diverse network of trusted foreign and domestic partners
- worldwide secure communications and logistics
- integration of human and technical operations (mutually supportive)
- effective security and counterintelligence program (keeps its operations and assets secret)
- mature mid-point collection
- integration of offensive and defensive missions (mutually supportive)
- comprehensive training program for all aspects of business

Figure 13 illustrates how an adversary possessing these capabilities can meet its offensive objectives across a broad spectrum of targets. A common misperception of the threat to information technology systems is based upon an adversary utilizing a small portion of the tools available to them. This is largely based on the everyday view of hacker-related exploits on the Internet. Unfortunately, an adversary has a very rich array of tools to use: surreptitious entry, spies, signals intelligence (SIGINT), clandestine technical collection, and cyber attacks. The synergistic and mutually supportive nature of these tools, in combination with the factors discussed above, can yield powerful offensive results.

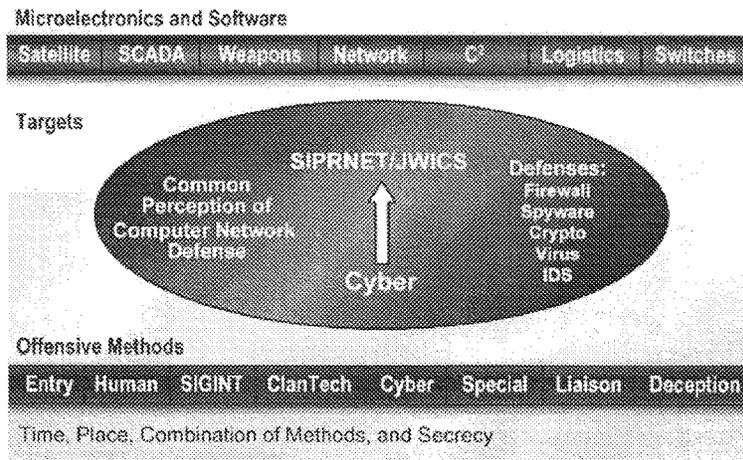


Figure 13. The Information Assurance Threat and Computer Network Defense⁹

⁹ For a more comprehensive treatment, see James R. Gossler, "The Digital Dimension," in Sims and Gerber, *Transforming U.S. Intelligence*, Chapter. 6, pp. 96–114.

With this context, the defensive challenges are daunting. New and well-resourced approaches must be developed to offset these offensive advantages. As will be shown, the innovative application of offensive techniques to support defensive objectives shows great promise.

The Insider Threat as a Priority Case. The information age insider threat can not only conduct espionage, the insider can also dramatically and broadly threaten the functionality of networks. It is important to focus on the insider threat as a priority, and ensure that the network quickly points at security violations by insiders.

Information Assurance Strategies. Maintaining an enduring, highly functional, and assured network-enabled environment is fundamentally strategic to managing the information, situational, support, and command dimensions of conflict in the 21st century. DOD will have total dependence on these networks for virtually every aspect of national security administrative and operational wartime tasks. The current mixed strategies of simultaneously working with COTS to reduce overall vulnerabilities (by increasing *protection*) while also strengthening monitoring, detection, analysis, and *responses* on the network may not be sufficient assurance in the face of the capable adversary, nor the best approach for the longer term. More detailed strategies need to be devised that *combine* offense, defense-in-depth, and deterrence and dissuasion options into combined effects for information assurance. Steps have been taken to think about and test the validity of these strategies in the context of now, next, and after-next temporal domains.

Defense-in-Depth. Defense-in-depth is the first line of defense against network vulnerabilities. The following lists the components of a credible defense strategy:

- strong leadership and governance oversight, processes, and investment
- a logically separate network (isolated from threats) to provide order wire, key distribution, and support for restoral functions
- run-faster acquisition that allows responsive and pervasive insertion of the latest COTS in order to present a constantly changing target environment to the adversary

- a robust and diverse set of government, industry, and academic R&D programs focused on high-leverage information assurance solutions and offerings such as identity, encryption, hardware and software assurance, security tagged architectures, and deep packet inspection
- hedging strategies and technologies for the future
- making the networks behave differently in combat
- protection of hardware and software supply chain
- establishment of a TargetNet/TestNet environment for designing, developing, testing, and exercising attack, defend, and exploit capabilities
- development of new security and sharing concepts that simultaneously maximize the provision of information while simultaneously protecting sensitive sources and methods

Deterrence and Dissuasion. Attacking U.S. information systems is undeniably attractive to adversaries. It represents the one chance to level the playing field, and if sufficient chaos is created, it can perhaps tilt the playing field in the adversaries' favor. All efforts must be orchestrated toward deterring any would-be opponent, mischief maker, or malicious bystander to execute such attacks, and if they do, ensure the ability to "fight through" and prevail. Adversaries need to be assured that their attacks against U.S. information systems will be detected, that U.S. functionality will be restored, and that there is the capability to operate securely with requisite system availability and integrity in degraded and wartime modes. More importantly, an adversary needs to know that the U.S. possesses powerful hard and soft-kill (cyber-warfare) means for attacking adversary information and command support systems at all levels. Deterrence and dissuasion strategies relate to:

- intrusion detection and attribution
- disproportionate response options and adversary consequences
- use of wartime modes
- managing the fight when under attack and operating in degraded modes

The utility of any information-managed net-centric system will be directly related to the confidence users have in the reliability and quality of the service. There is no approach that can guarantee that any system of the type being proposed and procured can be completely secure and all functions performed with 100% assurance. The price of introducing progressively higher levels of assurance is to induce greater cost and diminished functionality. It is inherently a risk management system of trade-offs and compromises for which there is no magic formula. *The greatest degree of assurance for the net-centric system that is being created can only be achieved by a balanced strategy.* A balanced strategy is one that places emphasis on sound defensive measures and an aggressive, sustained, and highly secure offensive program. The system that is sought will not have credibility with the users or potential adversaries if one is done without the other.

Every potential adversary, from nation states to rouge individuals, could be targets of an integrated offensive capability. Adversaries should be forced to invest in their own security, and should be compelled to consider the consequences of an attack on U.S. systems resulting in highly undesirable consequences to their own security. U.S. offensive penetration of an adversary's information systems, both offensive and defensive, is the essential ingredient in achieving an indication and warning capability.

Stratified Network Design

Intelligent Design

The network-centric information management system is based on the Internet design—initially the design of the ARPANET. It is a deliberately “flat” network. Every entity on the network—every node, every switch, every piece of subscriber equipment—has an IP address. This is a design that allows every communicant full access to their IP address. This is quite different from the model of the plain old telephone system where the telephone number is not yours to manipulate. In IP networks, subscribers can effect (and, thus, affect) the switching and signaling (the routing and/or apparent routing) of information. In other contexts, this attribute is referred to as “in-band signaling.”

Security and Control “Over-Net”

There are compelling reasons to want to take certain information and information services—network and security management services, in the broadest sense—out of band. That is, some things should be out of the grasp of subscribers, who have no legitimate need to touch them. The premise is that the most likely entry point for an evildoer is through the subscriber network, if, for no other reason than the “circle of trust” is bigger. Whether an insider or an intruder, the mischief should be localized with a substantial, additional barrier in the way of seizing, disabling, or corrupting the network. Other, more traditional processes, such as authentication and compartmentation, should limit the extent of any breach in confidentiality and, so, could profit from being less accessible to ordinary subscribers. Incidentally, it is likely that the underlying security services that enable identity management, also should ride the “over-net” and not the base subscriber net.

It is clear that the DOD, the original force behind the Internet, would be best served if such a stratified control layer used commercial equipment and software. More importantly, it would be most beneficial if the protocols became the (international) commercial standards, just as occurred with the Internet. In fact, it would be ideal if commercial service providers adopted the same control layer notion. It is, therefore, highly recommended that the developers work from the outset with major vendors and national and international standards bodies. In this sense, it’s believed that, having done it with the Internet proper, DOD can once again “invent COTS.”

The Information Assurance Battle Management Layer

Such a stratified network might also be used to manage the information assurance battle space, to provide situational awareness, command, and control of dynamic defense and, perhaps, offense—that is, a protective reactive strike. Some consideration might also be given to using such a network for the most critical command and control—nuclear, for example—or its backup and/or recall. However, caution should be applied: the more general-purpose this strata

becomes, the more nodes and users, and the more diversity, the more likely that it will lose its stratification.

Before extensive acquisition or deployment, a great deal of attention should be given to developing the concepts of operations for the layer. to flush out any serious information assurance concerns such as those expressed above. This should also allow for a decision to be made about how to operate the control layer—such as a layer for each level (JWICS, SIPRNET, and NIPRNET), or one control layer that restores, JWICS which, in turn, is used to restore SIPRNET, and so on. It is unlikely that one-control net acting across all three levels is desirable.

Elsewhere, it has been argued that the network is a critical combat system. This concept ties nicely to the notion that the stratified network control layer or security OverNet is the network battle management layer. As such, it should become an increasingly important part of the fight and should, therefore, be integrated into other command post functions. This will be especially true if there is movement towards an active defense of the network.

A good test bed might be the Army's Command Post of the Future, an executive level decision support system providing situational awareness and collaborative tools to support decision making. Situational awareness and key management functions should be accessible to a commander and fully integrated into his CIC. These network activities should integrate more like the way that logistics and transportation service providers integrate into the commander's business management space.

Information assurance is the high risk, long pole in the network enablement tent. Moving toward an acceptable level of assurance for DOD and related national security information is a supremely difficult and complex task. This area has been dramatically under-resourced, and the governance, oversight and organizational structures have been weak given the high stakes. There also needs to be a dramatically improved understanding of the threats and vulnerabilities by the users of the systems.

To achieve an acceptable level of assurance, red, blue, and green teaming needs to be strengthened. In addition, exercises, strong test and evaluation, and better concepts of operations need to be pursued. The success of such activities requires a viable and responsive, even an animated design, development and test environment, involving operators in activities where the network is degraded or non-functional, challenging restoral organizations with continuous wartime scenarios for managing the network in degraded modes and when under attack. DOD needs to ensure a holistic view of networks, so that the NII, joint, and agency programs of record are fully harmonized and synchronized with service programs, and those of the key allied partners. Equal attention needs to be paid to the plug and play nature of the applications layer, sitting on top of the services and transport layers for high speed insertion into the network, but ensuring expedited addressing of applications layer information assurance issues.

Architectures, Building Codes, Standards, Systems Engineering and Integration (especially at the enterprise level), Certification and Accreditation. Finding the proper balance of individual and collective focus and energy on each of these critical dimensions of network and information assurance acquisition is one of the most critical aspects of successful network design, development, and deployment. Deploying and continually upgrading operationally responsive network environments is the prime objective for DOD. A premium needs to be placed on maximizing the building codes, standards, advanced systems engineering, systems analysis, and the rapid certification of the information assurance aspects of network deployment.

Managing Partnerships. Relationships with DOD, the Director of National Intelligence (DNI), science and technology organizations, industry, laboratories, academe, and even foreign R&D organizations and activities need to be aggressively pursued and offered strong incentives. In particular, DOD needs to ensure that industry and academe have the requisite operational, network, and information assurance domain knowledge to make viable contributions in this strategic technology area.

Focusing on the Information, Information Sharing, and Security Reform. The DNI office has recently published an

Information Sharing Plan. The plan contains objectives, guidance, and processes, and stipulates actions, but does not describe specific detailed approaches and methods for maximizing sharing (while simultaneously protecting sources and methods). Providing better guidance on how information is to be shared will be the next major thrust of the DNI Information Sharing Office. It is important that such efforts be pursued aggressively, so that the information has assured delivery to all classes of customers, while the most sensitive aspects of the data are protected from both insiders and outsiders.

More important, information age challenges including information assurance require new security frameworks and thinking. The need to have a top level review of U.S. security policy and organization for the 21st century has been previously recommended by the Defense Science Board, as well as national commissions, but no national review effort has been tasked either by the executive or legislative branch. Such an effort is overdue.

Recommendations: Defense-in-Depth and R&D Agenda

Defense-in-Depth: Governance

- ASD (NII) should evaluate the information assurance funding over the Future Years Defense Program, focus on information assurance for the entire enterprise and increase current funding where appropriate.
- DOD CIO should establish responsibilities and authorities for end-to-end information assurance and security design.
- DOD CIO must formalize overall governance, systems engineering, and risk management enterprise-wide to focus on information assurance.
- STRATCOM and JFCOM should devise an information assurance battle management doctrine and tactics, techniques, and procedures.

Defense-in-Depth: Information Technology COTS Insertion

DOD CIO, ASD (NII), and USD (AT&L) must:

- Establish plans, policies and procedures for acquisition of COTS information technology systems from an information assurance perspective, which includes identifying and establishing information technology hardware and software provenance.
- Manage processes for rapid information technology insertion from a mission assurance and risk management perspective.
- Align and combine rapid acquisition processes and system engineering, certification, and accreditation activities.

Defense in Depth: Security Over-NET

ASD (NII) and USD (AT&L) should establish a defense-wide program to design, build, and operate an isolated network to improve GIG information assurance capabilities:

- hardening—out-of-band” critical signaling
- restoring trust—assured “order-wire” for reconstitution
- re-keying—assured critical key distribution

NSA, with DISA and the National Institute of Standards and Technology, should encourage commercial industry to incorporate new security architecture and design principles within evolving COTS networks:

- protocols and building codes
- international standards
- market development

Research and Development Agenda

DOD needs to cast its R&D net far and wide, and focus on those existing and potential high leverage information assurance solution areas, and move them more rapidly to the network market. The task force believes there are several powerful un-evolved areas that need attention:

DDR&E and STRATCOM develop research agenda to include:

- security usability
- self-aware networks
- adaptive networks
- detection and diagnosis
- deep packet inspection, intrusion detection system
- new design principles (resilience)
- hardware and software assurance
- static and dynamic analyses
- identity and access management
- formalized information assurance risk management
- security metrics
- encryption, public key infrastructure, digital signature
- security-tagged architectures, trusted platform model
- wireless security and performance
- dealing with adversary recovery of friendly information technology on the battlefield
- enhance information assurance at the data level

A classified annex to this report deals with certain aspects of threats, information warfare and information operations, wartime modes, making COTS behave differently, and hedging strategies and technologies for preventing exploitation of adversary recovered network components.

Chapter 5. A Critical Defense Weapon System

Combat operations, anticipated scenarios, and adversary actions require a new Combat Information Capability. This capability will be an enormous operational advantage for the war fighter. A CIC must be resourced, managed, and protected as a critical defense weapon system. Today information management systems tend to be managed more as a technology asset and curiosity than as a critical defense weapon system.

Commanders need to have the responsibility and authority that will allow them to take control of both their information and the associated infrastructure. Only after commanders are empowered can they move forward with developing the tools and processes to control this critical capability.

In addition to empowering commanders, there is a need to develop effective leaders that can lead in a net-centric environment. A net-centric leader must do more than simply be knowledgeable about information systems technology. They need to be leaders in the information age, which means they need to understand all aspects of how information can be used to provide a competitive advantage to their forces. One of the interesting aspects of unleashing information in an organization is that it will have the effect of flattening the organization, which usually creates a more rapid response entity.

One of the elements that need to come with a critical defense weapon system is an effective and robust training capability. The training cannot simply be to a fixed set of processes, but instead needs to focus on the principles of information management that will support flexible processes. This training needs to be connected with realistic operational exercises; therefore it is not simply an academic activity but one that will prepare the war fighters for combat.

In addition to the preparation of the personnel, another aspect of a critical defense weapon system is operational performance. Operational management must include the ability to monitor the status of the system, to establish operational priorities and trade-offs, to detect and deny intrusion, and evaluate performance based on a set of operational metrics.

Another element of a critical defense weapon system is the identification and development of the set of the tools necessary for daily operation. This set includes tools such as a help desk to support a wide range of users, tools for backup and restoration of the database, and network diagnostic tools. The combination of these tools with corresponding policies, doctrines, and procedures comprise a complete system operational management approach. Part of the day-to-day management of the system is the collection of new requirements that emerge from innovative uses of the tools. Many of these requirements can be satisfied with the development of new techniques and procedures. However, occasionally these requirements will require developmental activities. To accommodate both the emergent and new development requirements, an innovative governance and acquisition process must be put in place that will allow this CIC to keep pace with commercial technology. Instrumentation should be put in place to provide analysts the ability to monitor and understand how the system is being used and the impediments to reaching its full potential. Finally, in addition to a day-to-day systems management process, a longer term review process to assess progress and adjust strategic direction should be put in place.

Operating with Degraded Systems

Commanders at all levels must be prepared to operate with degraded information systems. Reduced network capacity may be the result of denial-of-service attacks or other combat actions. Corrupted data may be caused by network penetration or insider action.

For the tactical commander, operating with degraded systems (weapons, communications, logistics, maneuver) is not an anomaly but the norm. It is this defining quality of the tactical environment that requires modifications to the current deployment of net-centric

capabilities. Any solution to the challenges at the tactical level must start with the nature of the tactical environment and not the nature of the technical challenge. Two significant concerns voiced by tactical commanders when talking about leveraging the power of information fall into the category of redundancy and robustness.

The redundancy of the network and the critical data that rides on the network is a key attribute given the immediacy of enemy actions, the environment, and even unintentional errors. A practical, current understanding of how the various networks are working together and what options exist to restore or work around failures is a key requirement for commanders on a net-centric battlefield. Attention must be paid to the development of cueing capabilities to monitor and notify of intrusion and data corruption.

Robustness of the information systems employed is required for more than the obvious redundancy implied in the engineering sense of the term. A system that is robust will empower tactical commanders by instilling confidence that the information systems are every bit as capable as other tactical capabilities.

Commanders need cyber warfare capabilities to deal with an adversary's attempts to deny the unit's information capability. Defense operations require trained, skilled cyber warfare specialists and leaders who understand cyber warfare. The commander needs to take offensive cyber actions to protect the unit's capability and to adversely affect the adversary's capability. For example, the response to a penetration could be to steer the attacker into a honey pot for deception.

Commanders must develop concepts of operations; tactics, techniques, and procedures; and contingency plans to ensure that combat operations will continue with degraded information capabilities. Commanders need the necessary network status information to make risk-managed decisions about mode of operation, including available capacity, estimated extent of adversaries' penetration, corrupted information, prioritization of decreased capability, and implementation of planned degraded operations.

Combat units need to exercise regularly in degraded modes and use calibrated red and blue teams to understand the effectiveness of contingency plans.

Recommendation: Net Operations

STRATCOM must:

- improve the Joint Task Force-Global Network Operations center to world-class management capability
- develop and monitor performance and readiness metrics
- develop robust and redundant capabilities and operational procedures for information assurance
- enforce network management standards across the enterprise

Operators Need a System Test Environment

Operators need a realistic GIG architecture test environment to permit the testing of proposed new systems and applications, permit red and blue teams to examine potential attack and intrusions of the system, and test defensive and offensive information assurance approaches. This system must be capable of assessing the trades among performance, information assurance, and cost. It is recommended that the test environment include a range of options from virtual table top experiments, to simulation capabilities, to live real-world field exercises for operational testing and training.

Such a test environment has significant advantages of flexibility, speed, and completeness. It will permit system engineering analysis of the operational capability of the system under different configurations, with the addition of new commercial capabilities before they are added, and in degraded modes.

Recommendation: Test Environment

STRATCOM must establish a robust GIG test environment to examine the trades among performance, information assurance, and cost. Specific actions include:

- DOD CIO identify and prioritize emerging information technology and information assurance capabilities for testing.
- JFCOM create network operations and information assurance learning and training experiences.
- Combatant commanders conduct operational exercise tests and mission rehearsals.
- STRATCOM, NSA, and DISA validate and exercise a risk management system.
- STRATCOM and JFCOM identify and resource requirements.

Operate Effectively with Partners

One of the defining aspects of today's military environment is that it has moved well beyond simply joint service operations. Today's operations are fully integrated with key interagency, state, and local government; alliance; coalition; host nation; international; and nongovernmental organizations. Each of these actors generally operates on its own distinct network. Although sustained operations during the past decade in the Balkans, Iraq, and Afghanistan have led to the development of tools and arrangements for information sharing and collaboration, these efforts have typically been *ad hoc* and have not allowed for the true integration of all elements of national and international power.

Because future contingencies will almost certainly require the collaboration of U.S. forces with interagency, coalition, and nongovernmental actors, DOD must work to improve and institutionalize its ability to work effectively with partners in all stages of combat, stabilization, and reconstruction. CENTRIXS, for example, has been the vehicle for collaboration between U.S. and coalition forces during Operations Enduring Freedom and Iraqi Freedom. CENTRIXS

has been successful in many ways, but it is limited because it does not address information sharing with non-military partners, and it will not allow for U.S. and coalition forces to plan and operate on the same network. Although it is vital for operational security reasons that U.S. forces maintain this firewall between U.S. military networks and the networks of coalition and non-military partners, it is equally vital that the department work to find ways to improve the current situation in this area. Technical solutions will be helpful in this regard, but policy and process solutions are likely to be of equal or greater importance.

Recommendation: Interaction with Partners

DOD CIO develop policies and practices necessary for information sharing outside U.S. military (U.S. government agencies, allies, coalition, nongovernment organizations):

- clarify release authorities and amend as necessary
- define standards and best practices for information sharing and collaboration in both classified and unclassified domains
- provide for rapid stand-up of information sharing and collaboration following onset of a contingency

Critical Defense Weapon System

The most significant recommendation of the task force is for the Deputy Secretary of Defense to recognize the importance of the CIC as an essential combat capability and declare it as a critical defense “weapon system.” This means that the essential elements of the CIC will be planned, programmed, and resourced as a weapon system like other weapon systems. The CIC weapon system must be built to degrade gracefully when attacked. The assumption is that the GIG and the network operations to the HAIPE will be provided as planned and the weapon system, which includes support of the war fighter in the theatre, will be provided in a single portfolio.

This proposal is similar to the Air Force decision to recognize the Combined Air Operations Center and its extended elements as a weapon system. Then the manning, equipment, training, exercise, R&D, and other elements are programmed, planned, and resourced. The

consequence has been a more combat-ready capability and planned improvements over the period of the Future Years Defense Program.

A significant challenge will be to decide what programs will make up the weapon system elements. The communications and information management capability required in the battlefield should be part of the weapon system. The proposed information management support elements, such as combat information specialists, knowledge managers, and subject matter experts should be included. Particularly, the support for the war fighter outside the HAIPE should be included.

Given the scope and complexity of the total DOD information management system and its critical importance to U.S. combat capability, a comprehensive strategic plan is needed. This strategic plan is necessary to guide the development of a Combat Information Capability including:

- required resources
- timeline for key milestones for implementation
- addressing the major actions required to develop a Combat Information Capability
- training commanders to effectively command and control information management infrastructure and capabilities
- exercises and experiments for realistic operational scenarios
- information organization and access objectives
- doctrine for combat information capabilities
- a formal information assurance risk management system, model, and associated metrics
- education and training programs, including information management
- research on advanced information concepts
- lessons learned from current operations

This plan must be considered a living document and periodically updated as the threat, commercial technology, and other factors change that affect its capability and performance.

Because so much of the combat information requirement can be satisfied with existing and planned ISR capability, there is a need to develop a joint requirement for dynamic, integrated command and control of ISR assets. This capability can optimize the allocation of all ISR resources and lead to more robust sharing of tactical combat information. An essential part of building this capability is to incorporate the need for space platform visibility tools and ground segment improvements into this requirement.

Recommendation: Strategic Plan

The Chairman, Joint Chiefs of Staff should develop a CIC strategic plan that provides:

- commanders with the ability to command and control combat information capabilities
- staff capabilities to implement combat information management
- network operation, upgrade, and testing strategies
- experimentation, training, and exercises
- a formal information assurance risk management system, model, and metrics

Recommendation: CIC as a Critical Defense Weapon System

Deputy Secretary of Defense designate the Combat Information Capability as a critical defense weapon system.

Chapter 6. Conclusion

As this study evolved, it became clear that, given the way this system is to be fielded, *the Combat Information Capability must be treated as a critical defense weapon system*. It requires, therefore, a different mindset about how it is used, managed, and protected.

The evolving national security scenarios described earlier in this report demands increasingly distributed, dynamic operations. Whereas the network/COTS approach and strategy certainly enable new paradigms for sharing and using information, this capability also has the potential to significantly *increase* the nation's vulnerability to internal and external threats. It becomes a very attractive target for U.S. adversaries.

Therefore the task force members believe that the system and its capabilities will always be under attack and, as a result, will always be operated in either a degraded or compromised mode. Commanders need to understand this and know how to operate under this scenario. There are significant information assurance issues and risks that this CIC will be attacked, degraded, or compromised, and this risk must be resourced and managed accordingly.

One significant implication is the DOD needs a new, innovative acquisition strategy to take full advantage of the rapidly evolving capabilities of a true-COTS system.

The findings and recommendations of the task force can be distilled to three points:

- **DOD Combat Information Capability must be treated as a critical defense weapon system.**
- **Information assurance for this critical capability is critical and must be resourced and risk-managed accordingly.**
- **An innovative acquisition strategy is required to leverage true COTS information technology.**

Appendix A. Terms of Reference



THE UNDER SECRETARY OF DEFENSE
 3010 DEFENSE PENTAGON
 WASHINGTON, DC 20301-3010

MAR 15 2006

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT - Terms of Reference - 2006 Summer Study on Information Management for Net-Centric Operations

The United States military steadily transformed during the latter part of the 20th century by an ever increasing reliance on information networks and their ability to provide wider access to information and to support collaboration. Impressive gains in the usability, usefulness and availability of all forms of information have improved the effectiveness of military operations. Our increasing ability to leverage information and networking will be a critical enabling factor in developing better ways to work with others in the USG and with both coalition and non-traditional partners as we, collectively, undertake the challenging missions of the 21st Century.

Today a Company Commander can control a Division's worth of firepower, tagging and tracking systems promise to significantly improve the logistics chain and the improved availability of intelligence information and greater connectivity between sensors and shooters has increased the effectiveness of our forces and enhanced their security. During the past ten years, we have seen the evolution of military missions driven by adaptive adversaries who recognize our increasing dependence on information networks. Going forward, transformation must focus on addressing the stresses imposed by 21st Century mission challenges associated with stabilization and reconstruction operations in urban and unconventional environments and responses to unforeseen events with catastrophic consequences. Information and the ability that networks provide to make this information available to those who need it, as well as the ability for individuals and organizations to collaborate, are the lifeblood of military and civil-military operations. The quality, reliability, availability, timeliness, discoverability, relevance, and security of information and interactions among individuals and organizations across the enterprise (warfighting, with business and intelligence support) will have profound consequences for successful mission execution.

To date the transformation of the DoD enterprise has focused on improved connectivity, interoperability, and information sharing among disparate joint forces and systems. Future challenges and the need to maintain adequate levels of security, integrity, and reliability will place new demands on our information networks, processes and personnel. As new users demand more information and adaptive information sharing, improved knowledge utilization and better tools for information discovery will become critically important. "Googling" and "blogging" are making their way into military operations at all levels, but the full implications of this revolution are as yet unknown and we have no clear direction and defined doctrine.



You are requested to form a Defense Science Board Summer Study assessing the Department's strategy, scope and progress toward achieving a robust and adaptive Net-Centric DoD Enterprise.

The Summer Study should:

- Examine the operational value enabled by networks and networking and their impact on innovations across the Enterprise. Assess the implications of new and innovative approaches to command and control structures, capabilities, and processes, including interagency, coalition, and non-traditional participants, the need for greater adaptability and the emergence of new missions such as counter-insurgency, stabilization and reconstruction operations, counter-WMD, and catastrophic disaster support.
- Evaluate the underlying framework, architecture, processes and organizational structures that are in place or being pursued to deliver the power of information to the DoD enterprise as well as potential external partners. Explore Enterprise Wide cost/risk trades between bandwidth, quality of service, network availability, network security, information integrity, information sharing, and collaboration.
- Assess the state of the art in knowledge utilization. Particular attention should focus on information discovery, sharing in a secured networked environment, visualization and collaboration. How are emerging techniques being incorporated into operations both in the near and far term. How is information being turned into knowledge and then coordinated action as quickly as possible?

The study will be sponsored by me as the Under Secretary of Defense (Acquisition, Technology and Logistics) and the Assistant Secretary of Defense (Networks and Information Integration). Mr. Vincent Vitto and Dr. Ronald Kerber will serve as the Summer Study Task Force Co-Chairmen. Mr. John Mills, OASD (NII), will serve as the Executive Secretary. LTC Scott Dolgoff will serve as the Defense Science Board Secretariat representative.

The Task force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.



Kenneth V. Krieg

Appendix B. Task Force Membership

CHAIRMEN

Name	Affiliation
Dr. Ronald Kerber	Private Consultant
Mr. Vincent Vitto	Draper Laboratory

TASK FORCE MEMBERS

Dr. Milton Adams	Draper Laboratory
Dr. Shawn Butler	MSB Associates
Mr. Edward Carney	Cisco Systems, Inc.
Mr. John Dahms	Lockheed Martin
Dr. Craig Fields	Private Consultant
Mr. Scott Fouse	ISX Corporation
Mr. Greg Gardner	Oracle
Mr. James Gosler	Sandia National Laboratory
Ms. Carol Haave	Private Consultant
Mr. Richard Haver	Northrop Grumman
MajGen John Hawley, USAF (Ret)	CollaborX
Dr. George Heilmeyer	Private Consultant
Dr. Richard Ivanetich	Institute for Defense Analyses
LTG Keith Kellogg, USA (Ret)	CACI
Dr. William LaPlante	Johns Hopkins Applied Physics Laboratory
Dr. Robert Lucky	Private Consultant
Dr. Joseph Markowitz	Private Consultant
Dr. Mark Maybury	MITRE Corporation
Gen James McCarthy, USAF (Ret)	U.S. Air Force Academy
Dr. Jerry McGinn	Northrop Grumman
Dr. Dawn Meyerriecks	America Online, Inc.
Hon. Art Money	Private Consultant

Mr. Robert Nesbit	MITRE Corporation
Dr. Robert Popp	Aptima, Inc.
Mr. Lawrence Prior III	SAIC
Mr. John Quilty	Private Consultant
LtGen Harry Raduege, USAF (Ret)	Deloitte & Touche, LLP
Mr. Rocky Roccanova	Rock and Nova, Inc.
Mr. Larry Sampler	Institute for Defense Analyses
Hon. John Stenbit	Private Consultant
ADM William Studeman, USN (Ret)	Private Consultant
Mr. Alan Wade	Private Consultant
Mr. Kevin Woods	Institute for Defense Analyses

EXECUTIVE SECRETARY

Mr. John Mills	OASD-NII
----------------	----------

DEFENSE SCIENCE BOARD REPRESENTATIVE

LTC Scott Dolgoff, USA	Defense Science Board Secretariat
------------------------	-----------------------------------

GOVERNMENT ADVISORS

LtGen Bruce Brown, USAF (Ret)	ODoD CIO
Ms. Ann Carbonell	National Geospatial Intelligence Agency
Mr. Tom Gaetjen	JS J-6
Mr. Richard Hale	DISA
Mr. Mike Krieger	ODoD CIO
Mr. Robert Lentz	ODoD CIO
Mr. David Mihelcic	DISA
Ms. Cecilia Phan	JS J-6
Mr. Michael Ponti	OASD NII
Mr. Tony Sager	NSA
Mr. Thomas Scruggs	ODoD CIO

STAFF

Dr. Heather Davies	Strategic Analysis Inc.
Ms. Julie Evans	Strategic Analysis Inc.
Mr. Anthony Johnson	Strategic Analysis Inc.
Mr. Theodore Johnson	Strategic Analysis Inc.
Dr. Philippe Loustau	Strategic Analysis Inc.
Dr. Adrian Smith	Directed Technologies, Inc

Appendix C. Presentations to the Task Force

Name	Topic
------	-------

MARCH 20–21, 2006

Operator's Panel Group 1: COL Ralph Baker, Col Jagusch, MAJ Lynne Schneider, MSG Larry Riddle, Col Tucker, LTC Dave DesRoches Operator's Panel Group 2: LTC RD Douthit, LTC Sean Corrigan, MAJ Bob Castro, SGM Mike Hoover	Operators discussion panels
Mr. Ryan Paterson	Command Post of the Future
RDML Arther Brooks, NORTHCOM	Net-Centric Operations in Defending the Homeland and perspectives from Hurricane Katrina/Rita
Maj Gen Rajczak, JFCOM	Joint Command and Control
Mr. Mike Krieger, ODoD CIO	DOD Support for the Warfighter
LtGen Harry Raduege Jr., USAF (Ret)	Combat Librarian
Mr. Larry Huffman	DISA Support to the Warfighter

APRIL 20–21, 2006

Honorable John Grimes, Assistant Secretary of Defense for Networks and Information Integration	NII Overview
LtCol Joe Bessleman, Global Combat Support System (GCSS), Air Force MAJ Kurtis Warner, FusionNet Lorraine Wilson, Distributed Common Ground Systems (DCGS), Navy	Program of Record Perspective on Information Sharing Panel

Marian Cherry, Horizontal Fusion Edward Siomacco, Net-Centric Enterprise Services (NCES) Bernal Allen, Net-Enabled Command Capability (NECC)	Delivering Core Enterprise Services to Best Enhance Programs of Record
LtCol Steve Starks, USAF LTC Chuck Gabrielson, Army LTC Jim Garrison, Army Major Robert Wagner, Army CDR John Hearne, Navy	Technical Operators Panel
COL Ed Payne, Army, CIO-G6 LTC Harborth William, USA	Army Knowledge Online (AKO)
Kerim Tumay, VP Engineering Programs and Project Management	Convera
Tony Hall, Director, Factiva Global Government Sector Kirk Donval Homburg, Director of Service, Factiva Global Government Sector	Factiva
Kevin Laudano	Accenture

MAY 18–19, 2006

Craig Harber and Chris Kubic, NSA	Information Assurance Architecture
Gen James Cartwright, CDR USSTRATCOM	Discussion
Mr. Mike Krieger, OSD/NII	Data Strategy
Dr. Ron Jost, OSD/NII	Communications Architecture

JUNE 13–14, 2006

Dr. Linton Wells	Information Sharing with Non-Traditional Partners
Mr. Randy Cieslak, PACOM	TPIAS Phase III Data Flows
RDML Betsy Hight, USN	Joint Task Force-Global Network Operations
Terry Oxford-Scientific Advisor, NSA	Vulnerabilities to U.S. Critical Infrastructure

Mr. Paul Pittelli, NSA	Multi-Level Security
Mr. Ken Aull-Senior Technologist, ISD Office of Technology, Northrop Grumman Mission Systems	Identity Management
Will Kelchner- DIA	Defense Intelligence Multi-level Capability via MDDS
Mr. Donovan Lewis-Chief, Threat Analysis Division and Mr. Taylor Scott, DIA	Threats to the Network
Mr. Jim Gosler	The Digital Dimension
Sean O'Keeffe-Technical Director, Security and Evaluation, Office of Networks Solutions Engineering (C4), NSA/CSS Commercial Solutions Center	HAIPE Overview and MCEB—HAIPE Request for Joint Staff Assistance

JULY 18–19, 2006

MAJ Neil Khatod, USA-Chief of Concepts, TRADOC Program Integration Office — Networks and COL Jim Henderson, USA-Chief, Battle Command and Awareness Division, Army Capabilities Integration Center, TRADOC	Single Integrated Transport System
Dr. Larry Stotts	DARPA Tactical Communications
Mr. Mike Kern, Mr. Tony DeSimone, and Mr. Tony Modelfino, Assistant's to the Deputy to the ASD(NII)/DOD CIO, for Enterprise Wide System Engineering	Enterprise engineering issues and performance assessment approach example for quality of service
Dr. Robert Popp and Dr. Craig Haimson	Last Tactical Foot
Mr. John Landon	NII Acquisition

AUGUST 9, 2006—INDUSTRY PERSPECTIVES

Mr. Bill Clingempeel	Qualcomm
Mr. George Spix	Microsoft
Mr. Bob Shrimp	Oracle
Mr. Rafat Alvi	Sun
Mr. Greg Akers	CISCO

Appendix D. Glossary

ASD (NIJ)	Assistant Secretary of Defense for Networks and Information Integration
C2	command and control
CIC	Combat Information Capability
CIO	chief information officer
CONUS	continental United States
COTS	commercial off the shelf
DDR&E	Director, Defense Research and Engineering
DISA	Defense Information Services Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DSB	Defense Science Board
EWSE	Enterprise-Wide System Engineering
GIG	Global Information Grid
GIG/BE	Global Information Grid/Bandwidth Expansion
HAIPE	High Assurance Internet Protocol Encryption
HUMINT	human intelligence
IM	information management
IP	Internet Protocol
ISR	intelligence, surveillance and reconnaissance
JCIDS	Joint Capabilities Integration and Development System
JFCOM	Joint Forces Command
JTRS	Joint Tactical Radio System
JWICS	Joint Worldwide Intelligence Communications System
NCES	Net-centric Enterprise Services
NCO	network-centric operations
NECC	Net-enabled Command and Control
NIPRNET	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
POP	point-of-presence
R&D	research and development
SIGINT	signals intelligence
SIPRNET	Secret Internet Protocol Router Network
SRW	soldier radio waveform
STRATCOM	United States Strategic Command

TMOS	TSAT Mission Operations System
TSAT	Transformational Satellite Communication
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
WIN-T	Warfighter Information Network-Tactical
WNW	wideband networking waveform

352

*Defense Science Board
2006 Summer Study*

on

**Information Management for
Net-Centric Operations**



*Volume II
Operations Panel Report*

April 2007

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This supporting paper of the DSB 2006 Summer Study on Information Management for Net-Centric Operations contains material that was provided as inputs to the volume I report. The findings and recommendations contained herein may not represent the consensus view of the full study.

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

The DSB 2006 Summer Study on Information Management for Net-Centric Operations completed its information gathering in August 2006.

This report is UNCLASSIFIED and releasable to the public.

Table of Contents

Chapter 1. Introduction.....	1
Chapter 2. Deriving Information Needs from Operational Scenarios.....	6
Chapter 3. Combat Information Capability.....	15
Chapter 4. CIC Functions and Staff.....	26
Chapter 5. Tactical Operations.....	41
Chapter 6. A CIC is a Critical Defense Weapon System.....	54
Chapter 7. Major Recommendations.....	69
Appendix A. Terms of Reference.....	73
Appendix B. Glossary.....	76

Chapter 1. Introduction

Operations Panel

Panel Co-Chairs:

Gen Jim McCarthy, USAF (Ret), U.S. Air Force Academy
LTG Keith Kellogg, USA (Ret), CACI

Members and Government Advisors:

Mr. Scott Fouse, ISX Corp
Mr. Greg Gardner, Oracle
MajGen John Hawley, USAF (Ret), CollaborX
Dr. Richard Ivanetich, IDA
Dr. Jerry McGinn, Northrop Grumman
Mr. F. Michael Ponti, OASD NII
LtGen Harry Raduege, USAF (Ret), Deloitte
Mr. Kevin Woods, IDA

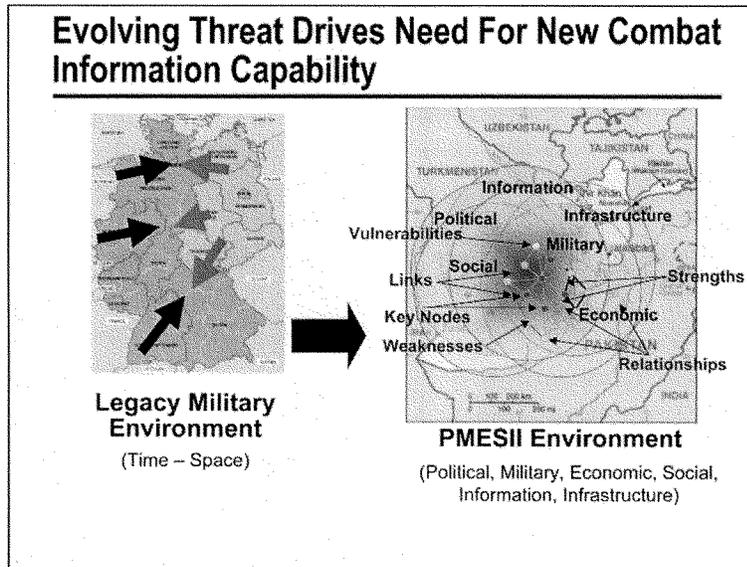
This report of the operations panel of the Information Management summer study served as the basis for the full summer study report sections that included warfighter assessments of needs and suggested improvements to enhance combat capabilities. The panel appreciates the candor and insights that formed the basis for panel recommendations. The panel co-chairs acknowledge the investment of time and the insights that the panel members brought to this study.

The panel contributed primarily to the first and fourth statements in the terms of reference.¹ The panel examined the operational value enabled by information networks. Particular attention was paid to

1. The study's terms of reference is Appendix A.

emerging missions, counterinsurgency, counterterrorism, stabilization and reconstruction, and response to catastrophic disasters. The panel assessed the state of knowledge management for information networks. Additionally the panel focused on information discovery, sharing, collaboration, visualization, and storage for all missions and users. In addition, the elements of a Combat Information Capability (CIC) were developed and described.

The panel's principal focus was on warfighter's needs as viewed through the eyes of those who experienced combat operations in both Iraq and Afghanistan. This perspective helped the study members appreciate the value of a CIC both as kludged in today's combat environment and desired for the future.



There are a number of catalysts for change. These include globalization, the information revolution, and force changes in structure and technology.

In terms of globalization, the environment has evolved from a relatively immature state where, in the industrial age of the 20th century, security meant “defense” and “containment;” to a more mature and integrated environment where “the world is flat,” information is shared globally in near real time, and where security means “defense and all else.”

The information revolution has moved the world from a place where data moved at about 30 words per minute over field phones and 60 words per minute over radios to one in which data can be moved at roughly 1.5 trillion words per minute over wideband data links. The impacts on the U.S. security environment are enormous.

There are other evolving threat characteristics that the panel considered during the course of the study. Future threats will be:

- dynamic and ever changing
- highly mobile and regularly move across international borders
- highly distributed
- stealthy
- adaptive and amorphous
- asymmetric
- and, when viewed in isolation, low value targets

Adversaries have become very skilled at neutralizing U.S. operational advantages. Of primary concern to the study was that U.S. adversaries seemed to not only be using their many skills in information technology to move information rapidly, but also they have a significant capability to attack U.S. information systems. There was also much concern expressed about the trend of commercial-off-the-shelf information technology production moving to Asia and the implications of this trend.

Since Operation Desert Storm, the United States has reduced the size of its warfighting forces by 200 ships, 12 air wings, and 4.5 divisions. At the same time:

- There are more active and potential global hotspots.
- The threat is increasingly using asymmetric tactics.
- Interoperability is still an issue with many coalition and allied participants not to mention inter-service.
- Long-term allied support is not a given.

A fundamental trade of massed forces for massed electronics has occurred. The defense budget has remained flat with investments focused more on information technology; precision; command, control, communications, and computers; and intelligence, surveillance, and reconnaissance. Now, there is a need for rebalance so that the investment focuses on making sense of sensor information.

The implication is clear: technological advances and radically improved collaboration and information sharing capabilities with smaller, deployable military forces mandate interdependence across the range of national power (political, military, economic, social, infrastructure, and information). It also places a premium on managing information and making the right decisions at the right time.

In a practical and logical sense, this environment means that the government will have to be more effective at convincing the population of a target country (Iraq, for example) to support their government and refrain from violence in order to promote economic pluralism, restore and improve infrastructure services, and promote legitimate governance within a context of full spectrum information operations rather than just simply training their security forces and conducting military operations against insurgents.

This dynamic frames the outlook on security operations in the information age.

Chapter 2. Deriving Information Needs from Operational Scenarios

Operational Observations-Warfighter Panels

- Focus: ISR and command and control supported by information management
- Complex distributed, ad-hoc operations require new information management and command and control concepts
 - Information management services for disadvantaged users
 - Dynamic management of distributed ISR assets
 - Appropriate information assurance and security
 - Operations with degraded networks
 - Operations with coalition partners, non-government organizations, other agencies, and state and local governments
- Significant frustration at tactical level with limited communications, information sharing, collaboration, and discovery capabilities
 - Personal cell phones
 - Chat rooms
 - Web search

} ad-hoc solutions flourish
funded by supplemental budgets

The focus of most combat operations over the past several years has been overwhelmingly in the land domain. The distinguishing characteristic of this domain, with some exceptions, is its people-centric nature. This characteristic is distinct from the platform-centric nature of other domains or even more traditional conventional land combat. The recent experiences of warfighters in the tactical environment, employing the currently fielded net-centric capabilities, provides the department a critical opportunity to validate the theory and promise of information and networks at the tactical level. The validation of the network-centric operations thrust of current

Department of Defense (DOD) activities should also include a serious look at its risks, vulnerabilities, and challenges.

Warfighters are singularly focused on capabilities that help them achieve their assigned missions. Sophisticated information capabilities introduced in the past several years have made a significant impact on the tactical battlefield. On the positive side, the ability to share, communicate, and collaborate on vast amounts of information is changing the way some commanders organize forces for combat. On the negative side the tactical networking solutions continue to be ad hoc in nature. In some cases, the solutions to capability shortfalls are solved by adapting commercial capabilities outside programs of record. In other cases, it is adapting programs of record through the use of civilian networking concepts like web chat.

The observations of several warfighter panels varied according to the particular experiences of the participants. Nevertheless, several findings emerged. Information management was the warfighters principal concern. Finding the needed information effectively and in a timely manner was very difficult for both the tactical commander and the staff. The information management challenge at the tactical level was couched in very practical terms: warfighters want information management concepts that support, not restrict, their concepts of operation. Commanders want improved access to intelligence, surveillance, and reconnaissance (ISR) data at all levels. In some cases, this access is desirable without value-added analysis; in other cases, intelligence processing is helpful as long as it meets time requirements. Establishing information sharing and collaboration seamlessly for voice, data, and video without regard to organizational echelon is the desired end state.

Operational Scenarios

- Prevent and protect the United States against catastrophic attack
- Conduct large-scale counter-insurgency operations including stabilization and reconstruction
- Conduct global distributed, small-scale operations including counter-terrorism and humanitarian relief
- Enable large-scale operations against near peer adversaries

**All scenarios require a new information management capability
A technically capable adversary will likely attack the system**

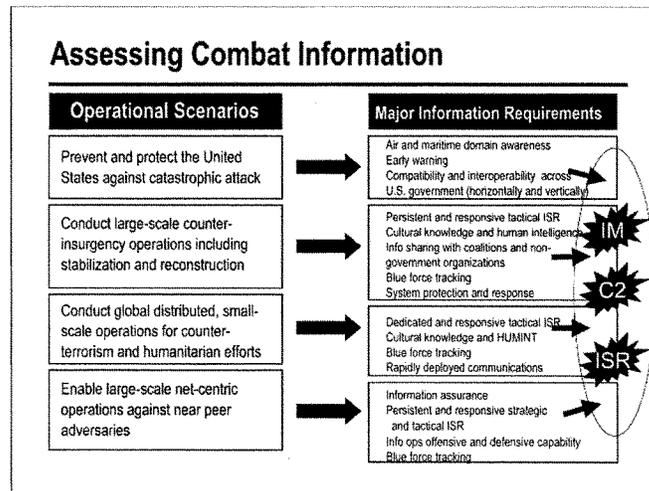
The study assessed the following operational scenarios that were derived from the threat assessment prepared for the most recent Quadrennial Defense Review:

- prevent and protect the United States against catastrophic attack
- conduct large-scale counterinsurgency operations including stabilization and reconstruction
- conduct global distributed, small-scale operations including counter-terrorism and humanitarian relief
- enable large-scale operations against near peer adversaries

It was concluded that under all scenarios a sophisticated and state-of-the-art information management capability would be required.

Information systems technology has proliferated across the globe driven primarily by the global economy and the Internet. One could argue that the United States no longer holds a significant advantage in information systems technology. Potential adversaries are technically

very capable in this area and are able to move information rapidly. Adversaries will also clearly understand the importance of information to winning in combat and will therefore commit to attacking U.S. command, control, communications, and information systems. These attacks may be kinetic and/or non-kinetic attacks.



When the four operational scenarios are examined in detail, certain major information requirements become clear for each scenario. These information requirements include data, capabilities, and tools that would facilitate success in each of the respective scenarios. These needs are by no means exhaustive, but the ones listed below are illustrative of the respective scenarios and they provide a good sense of the types of information required for today's security challenges.

Prevent and protect the U.S. against catastrophic attack

- air and maritime domain awareness
- early warning of potential attacks against the United States
- compatibility and interoperability across the U.S. government, horizontally and vertically (that is, at the federal level among various agencies and departments as well as between federal, state, and local authorities)

Homeland Defense

Conduct large-scale counter-insurgency operations including stabilization and reconstruction

**Iraq
Afghanistan**

- persistent and responsive tactical ISR, for example, to track small groups and counter improvised explosive devices
- cultural knowledge and human intelligence to gain an understanding of the local environment
- information sharing with coalitions and non-government organizations to harmonize mutually reinforcing efforts
- blue force tracking to maintain situational awareness and prevent fratricide among U.S. and coalition forces
- system protection and response

Conduct global distributed, small-scale operations for counter-terrorism and humanitarian efforts

**Horn of Africa
Philippines**

- dedicated and responsive tactical ISR, for example, to track small groups and support deployment of humanitarian assistance
- cultural knowledge and human intelligence to gain an understanding of the local environment
- blue force tracking to maintain situational awareness and prevent fratricide among U.S. and coalition forces
- rapidly deployed communications

Enable large-scale net-centric operations against near peer adversaries

China

- information assurance
- persistent and responsive strategic and tactical ISR
- information operations offensive and defensive capability
- blue force tracking

This examination shows that, while there is much commonality across the scenarios, the major information requirements have needs that are distinct for each operational scenario. Nonetheless, three major areas emerge as central throughout all of the scenarios:

- information management
- combat information capability command and control
- intelligence, surveillance, and reconnaissance.

Moreover, information management, command and control, and ISR—taken as a whole—combine to form what the panel termed a “Combat Information Capability,” a term that will be defined and developed in the subsequent discussion.

There are significant capability shortfalls in these areas that need to be addressed. These gaps will be discussed on the following pages.

Operational Gaps to Maximizing the Value of Information

- Information management
 - No assured access to critical data stores in reserve
 - Tools are inadequate to monitor and control networks
 - No automated solutions that facilitate information sharing with non-DOD partners
- Command and control
 - Inadequate communications at tactical levels
 - Data/network overload hampers timely and effective decision-making
 - Capability to conduct cyberwarfare
 - Inadequate staff and tools appropriate to the information realities at the tactical level of war
- Intelligence, surveillance, and reconnaissance
 - Present combat information and ISR systems are not configured to gain full advantage of their capability
 - Access to combat information and ISR data requires special applications and training to make that information usable
 - There is not a unified management concept to bring multiple sensors against a high priority target or to optimize broad area coverage with all available assets
 - Many battlespace entities are unidentified and/or locations are ambiguous

After discussions with a cross-section of warfighters with recent operational experience in Iraq and Afghanistan, as well as insights from panel members, three areas of concern emerged: information management, command and control, and ISR.

Information management. Recent operations have reinforced the endemic challenge of providing the right information at the right time in the right form. The ability of commanders to organize and manage information and related resources was limited by a host of complex interrelated issues. The most common refrain was visibility, access, and flexibility. In general there is a significant gap in the ability to manage combat information, which includes the process of identifying, collecting, organizing, making available, assuring the quality of, and protecting information for operational use. Information management will provide essential mission functionality for the user to discover (data and services), understand, and use information, and collaborate with other users.

Command and control. In this context command and control is defined within the scope of activities generally associated with information. Commanders at all levels recognize the need to understand the critical capabilities necessary for mission success. Many of the warfighters realize that “control” of assets is not the crucial issue. The challenge is a fundamental lack of ability to see, understand, and influence critical issues such as bandwidth, ISR management, and information sharing with coalition partners.

ISR. The tactical warfighter’s major concern was the inability to access or fuse ISR data. The ISR data being referred to would include the full range of sensor outputs to include human intelligence reporting.

The often repeated statement “every soldier is a sensor” is meaningless unless the flow of information is two way and accounts for the nature of the environment in which the information is useful. Data collected at and for the ground tactical level (complex physical and human terrain) is, by its nature, incredibly cluttered. The nature of operations in this environment (ambiguity, time constraints, and lack of mobility, for example) means that the sensors generally, when compared to those in a platform-centric environment, tell a commander less and then only after more processing.

Chapter 3. Combat Information Capability

Improving Information Management, ISR, and Command and Control in a Net Centric Environment

- Need more responsive and informed decision making with more rapid and wider sharing of information, enhanced presentation
- Need improved situational awareness drawing on wider information sources and shared understanding (e.g., CPOF)
- Need enhanced and more timely planning resulting from greater collaboration and increased parallel activity
- Need improved synchronization in mission execution resulting from increased coordination among distributed forces

Conclusion: Need a “Combat Information Capability”

To draw the most combat capability from a net-centric environment, information management, ISR, and command and control must be improved. Decision-making must be conducted more rapidly, with wider information sharing and enhanced means for presenting material. Tactical forces need improved situational awareness by drawing on a wider base of information sources and benefiting from improved and shared understanding. An example of this philosophy in action is the Army’s Command Post of the Future. Operational planning needs to be improved through greater collaboration among applicable participants. The warfighter needs time-saving benefits derived from increased parallel activity and less reliance on old, slow serial processing. Mission synchronization needs to be improved through increased coordination among distributed forces. In short, different ways of thinking about the criticality of battlefield information are required. Today, DOD needs a Combat Information Capability for modern military operations.

What is a Combat Information Capability?

- **Foundation:** the Global Information Grid (GIG) extended securely as far as possible into the tactical arena
- **Protection:** GIG protected against adversaries and disruption/penetration and provide capability for reconstitution
- **Command and control:** ability of the commander to dynamically control and defend his combat information capabilities
- **Collaboration/information sharing:** optimizing effectiveness of and interdependent joint, interagency, and multinational force
- **Combat information management:** analyze/process information to support decision-making
- **Services:** provide raw information to support combat operations
- **ISR:** allocation of sensor and analysis capability to optimize combat effectiveness
 - Includes "soldier as a sensor"

The concept of a CIC becomes the commander's primary enabler for providing command and control of military forces. This includes new ways for maintaining oversight of forces, sensors, networks, and the information flowing to, from, and within the battlespace. It is envisioned to have the seven characteristics shown above.

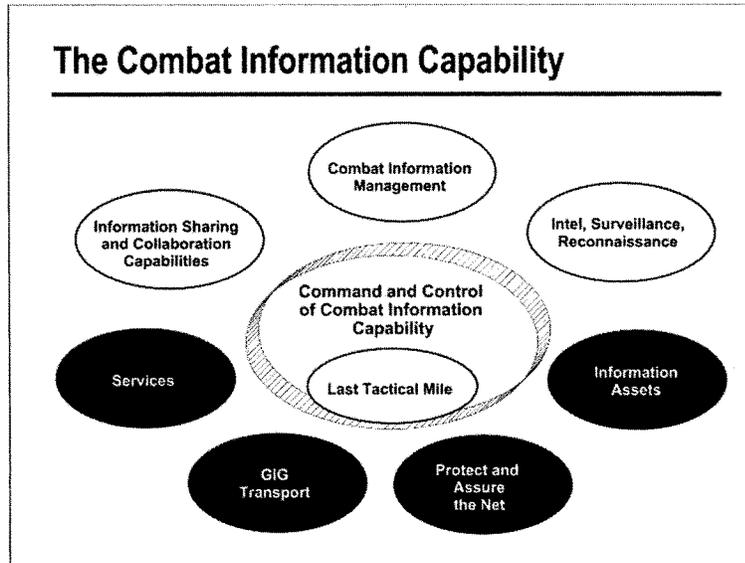
A CIC will collect and disseminate authoritative location and identification information on battlespace entities, targets, and threats; facilitate information sharing and collaboration; support critical operational and logistics planning; and provide improved situational awareness and understanding to decision makers.

The bottom line is that soldiers walking through the Shia-Kot Valley in Afghanistan during Operation ANACONDA who took fire from Taliban forces hidden in a cave want net-centric operation and self-synchronization capabilities, and want it right here, right now to make the adversary go away.

If they are networked, they can share their situational awareness and their very high fidelity perspective of the battlespace with those that may not have the same perspective, such as the low flyers who have a moderate fidelity perspective, or the high flyers who have a low fidelity perspective. If the situational awareness and perspective across participants and platforms can be shared, then those participants will be able to quickly collaborate on the desired effects needed and decide on the best capability in which to engage. Commanders don't want tens of bombs from a B-52 if, for example, friendly forces are only hundreds of meters away.

On the other hand, if the ground forward air controller and F-16 pilot share a picture of the situation (shared situational awareness) they are able to quickly collaborate and decide on what to do when the situation dynamically changes. In other words, they self-synchronize to best engage the enemy and avoid fratricide.

There is, however, a quality aspect to information in this net-centric environment. Consider, for example, the video clip used by insurgents in Iraq to demonstrate that Americans were indiscriminately bombing civilian crowds. Information was taken from a sensor, manipulated, and broadcast as truth. This example emphasizes that higher quality information needs to be rigorously cross-checked for accuracy.



The CIC can be described by referring to the chart above. The foundation is the global information grid (GIG) transport extended to the High Assurance Internet Protocol Encryptors (HAIPE) that are to be moved as far forward as possible and include information assurance elements of the network. This design is intended to provide wideband capability with robust defenses. The elements that will “protect and assure the network” assume that adversaries will attempt to deny this important capability.

“Information assets” refer to data that is generally stored in data sources available to the warfighter. Sensor data, track data, and analyzed information would fit into this characterization. “Services” are the tools that permit discovery and exploitation of the data, applications, displays, and persistent collaboration capability to satisfy combat information needs. Depending on the scenario, the GIG, information assets, services, and the protect/assure functions can be separated from the normal business of the department to attain a higher priority, greater assurance, and security, and more secure data bases and services by parsing.

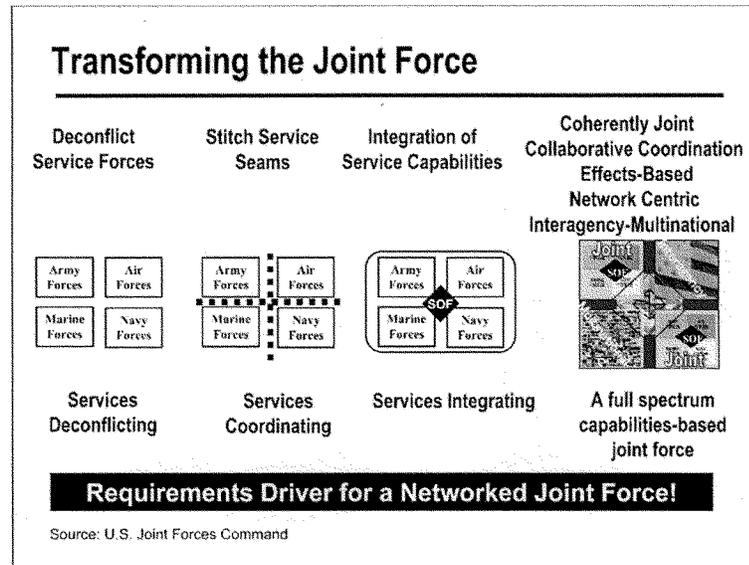
The gray areas on the chart are focused on the operational and tactical level of operations and the recommendations to improve capabilities over the last tactical mile. “Combat information management” refers to strengthening the structure to provide commanders and individual warfighters with educated and trained assistants who understand and support combat information requirements. An “information sharing and collaboration” capability refers to the tools and communications that provide the ability to share information dynamically and to collaborate for planning and execution.

Command Post of the Future (CPOF) capabilities in Iraq are an excellent illustration of the value of collaboration that is explained later in the report. “Intelligence, surveillance, reconnaissance” refers to the ability to treat operational and tactical ISR assets as an ISR “system” to obtain the most effective, responsive coverage by limited assets. The data flowing from ISR assets may be made available simultaneously to the user and to the analyst.

To achieve maximum combat effectiveness, the commander must be able to control this warfighting capability as is done with other essential elements of combat power. This report describes aspects of the CIC that permit the commander to exercise command and control.

The “last tactical mile” generally lies outside the HAIPE, may have limited communications bandwidth, has unique security and assurance requirements, and warrants particular focus in this study. The panel outlines particular requirements to support the “disadvantaged” warfighter.

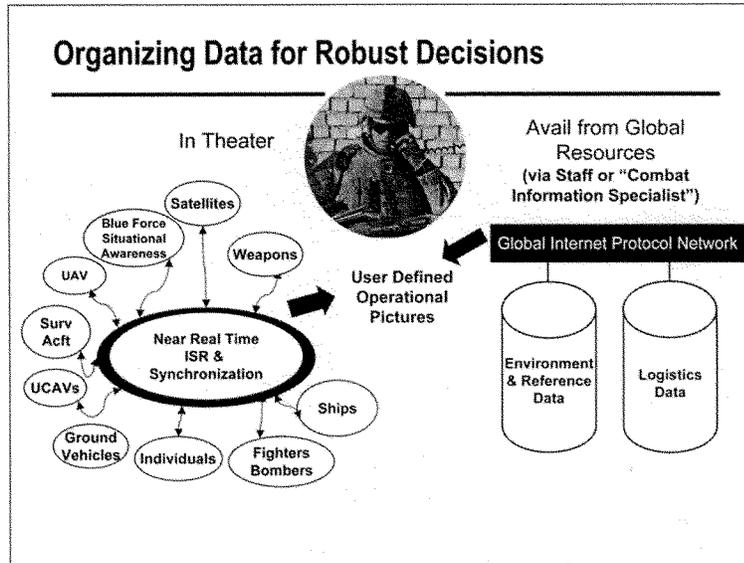
Taken together, these elements comprise a CIC that the report will outline as its principal finding.



It is important to understand how joint forces will be employed before the design of the CIC is finalized. The figure above is an illustration that was created by Joint Forces Command to show the history and future of joint force operations. In the not too distant past, joint force commanders could only reliably disseminate written orders to subordinates and, thus, had to employ procedural means of deconfliction such as lines on the battlefield and/or time deconfliction to insure safe separation of component forces. For example, in the Vietnam era, Air Force units were employed in the Hanoi region by day but by night Navy forces were used in order to prevent the potential for fratricide. Gradually, as battlefield communications began to improve, joint force commanders were able to start employing component forces in closer proximity to one another. New concepts such as joint engagement zones were developed to more closely integrate the joint force. The Joint Fires Initiative was a key part of Millennium Challenge 04, a recent major joint force experiment.

The operational goal for the future is to be able to conduct interdependent joint operations where any sensor under the control of any joint component commander can sense any other components' targets. This sensor would provide target quality information to that component so that the best available weapon from any component or service can be employed against almost any target on the battlefield within range. Sometimes this is referred to as the "any sensor, any weapon" concept. Thus, joint interdependent operations is a concept that allows the joint force commander to achieve an effect against an adversary using the best system (or sensor) available irrespective of operational command of assignment. Under joint interdependent operations, when a time-sensitive target emerges on the battlefield, the commander in charge of joint force employment will be able to attack the target with, for example, an aircraft, naval gunfire, and/or ground artillery, depending on which asset can be brought to bear in a timely manner and have the desired effect on the target.

The key enabler to being able to operate in the manner described above is creation of an unambiguous track data environment of all battlespace entities (friendly, enemy, and neutral) that can be simultaneously shared at all levels (strategic, operational, and tactical) via user-definable operational displays. This capability is sometimes referred to as a single integrated picture of the battlespace. The figure on the next page is an illustration of how the single integrated picture, as a key element of the CIC, will be created and disseminated.



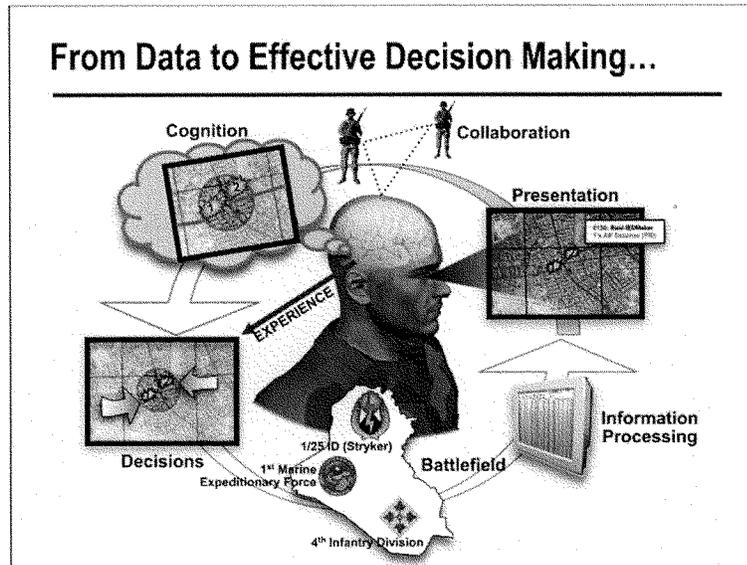
Command centers at both the strategic and operational levels, as well as tactical joint force elements, must have a common understanding of the location and identification of all battlespace entities (people, air vehicles, ground vehicles, ships, subsurface vehicles, space vehicles, buildings, bridges, critical infrastructure components). This information comes from a variety of sources, many of which are represented in the ovals on the left side of the figure above. Under the concept of a net-centric force, it is envisioned that these sources will be networked and integrated together in such a manner that precise tracking and identification of all battlespace entities will be achieved.

It should be noted that some key work is already underway in the department, under the auspices of the Joint System of Systems Engineering Office, to integrate sensor inputs to achieve unambiguous air track data so that a single integrated air picture can be created. Experts advise that the same software engineering approach that is being employed to create an unambiguous air track data environment can also be employed for the other domains (such as land, maritime,

space, and, perhaps, cyberspace) thereby creating an unambiguous track data environment for all domains.

This unambiguous track data environment created primarily via a well-synchronized, near-real-time ISR tracking network (illustrated in the figure above) will then become a key information source that can be shared across all joint force elements via the GIG. The information from this key CIC data source, as well as information from the other data sources shown above, can then be displayed by joint force elements (users) in many different ways and on varying scales via user-defined operational displays. The user-defined operational displays needed at the tactical level may vary significantly from those required in a command center. However, the important premise is that all user displays use common data sources so that the information is consistent and authoritative across the entire joint force.

The net effect is that the warfighter will have near real-time data and the user-defined operational display to carry out the assigned mission.



Once the information is made available to the user, the next major problem to address is how to support that user in making sense of that information.

The answer lies in net-centric operations theory as articulated by, among others, Garstka and Alberts. This theory addresses physical, information, cognitive, and social domains. The physical is where strike, protect, and maneuver take place across the environments of ground, sea, air, and space. The information domain is where information is created, manipulated, added value to, and shared. It can be considered the “cyberspace” of military operations. The cognitive domain is where the perceptions, awareness, understanding, decisions, beliefs, and values of the participants are located. These intangibles are crucial elements of network-centric operations. The social domain is where force entities interact, exchanging information, awareness, and understandings, and making collaborative decisions. It overlaps with the information and cognitive domain but is distinct from both. Cognitive activities by their

nature are individualistic; they occur within the minds of individuals and are, therefore, the heart of decision-making.

Chapter 4. CIC Functions and Staff

Combat Information Capability Includes: Innovative Approaches for Combat Information Management

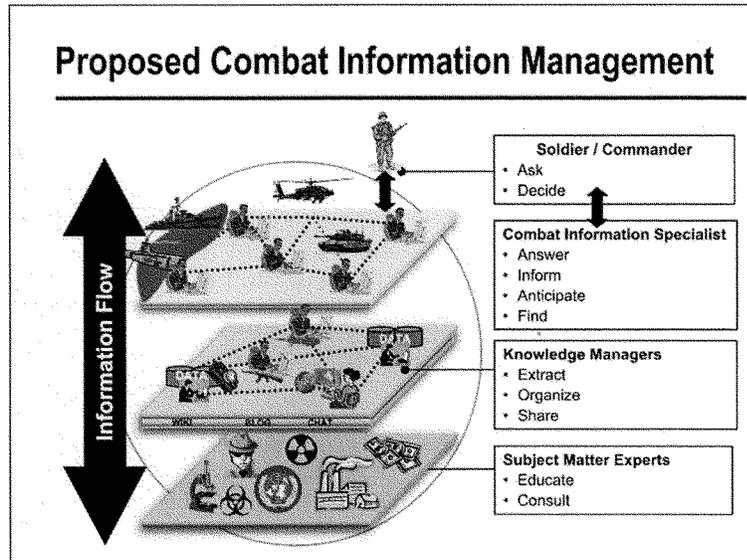
- Flag level combat information support staffs to ensure that needed information is made available in the right form
- Combat information specialist to provide timely and tailored information to the warfighter at the tactical level
- Combat information integration tools to support operational commanders
- New devices that allow the warfighter to access and provide information while maintaining their own situation awareness

Getting information to the commander or warfighter is necessary and challenging, but by itself insufficient to enable making the best possible decisions and employing forces to the best effect. To achieve that end, the commander needs focused practical assistance in processing information. At the brigade level and above, commanders need a specific, focused staff to process information into a form that enables better decision-making.

Importantly, the panel believes that commanders in the rank of O-9 and above (those who serve as joint force commanders) need a dedicated combat information integrator to optimize their ability to make effective, timely decisions. The combat information integrator facilitates collaboration and information sharing; ensures disciplined information

management; facilitates interdependence among diplomatic, information, military, and economic partners; blends the art and science of information management; and leverages best practices. This individual has a number of key attributes: significant and relevant operational experience, commander's trust, exceptional intellectual curiosity, and technological sophistication, and undergoes continual training. The combat information integrator is appropriately empowered to interact with commanders and is managed via a unique career management path.

The following pages describe a new management approach to information which includes staff functions, tools and training to assist commanders in assessing situational awareness, system operating mode, force allocation, and ultimately making better decisions.



Combat information management involves the seamless, timely flow of information between and among a globally connected set of players. At the tactical level, individual soldiers and commanders, who are often bandwidth-constrained, rely on organic combat information specialists to help them access, analyze, and process information for decisions. Those specialists are connected with specially trained and experienced knowledge managers, probably operating from a geographically distant location, who provide additionally refined and detailed information, upon which decisions can be made. Importantly, these knowledge managers are content experts, not staff officers.

In turn, knowledge managers access national or international level subject matter experts, who provide deep expertise in designated fields. When appropriate, subject matter experts work directly with combat information specialists to provide timely, refined information to combat commanders to make better informed decisions. This system is fully interconnected and “flat,” and global information flows horizontally and vertically among these experts who focus solely on this function. Information flows up as well as down—subject matter experts are

informed by the latest tactical developments as much as they help combat information specialists.

To date there has been an overall lack of focus and effort on managing information in the GIG, including its creation, quality assurance, access control, and timely and appropriate dissemination. Commercial industry, especially those involved in businesses where a “knowledge advantage” provides a critical competitive edge, recognizes the value of information and invests in systems and people to exploit it. For example, Accenture (Accenture.com), a \$15 billion global management consulting and technology services company, recognizes that their information base and experience is their most valued corporate asset and they treat it as such. They assign more than 150 information managers (called knowledge managers) to functional specialties, such as oil, gas, insurance, and pharmaceuticals. Information managers collect, process, and disseminate to interested parties the latest and most important information in their domain. They know the most relevant sources, the best subject matter experts, and identify the best practices in their focus area. They are responsible for both quality and content of information in their domains. They ensure that the full company’s knowledge base is available to their field representatives who interface with customers. Their focus is on the information and its management, not on the technology for its storage and delivery—though they rely heavily on an effective technical base.

Current DOD doctrine does not explicitly recognize the management of combat information as a critical military resource. Accordingly, the military services and combatant commanders need to establish combat information positions and associated concepts of operations. The figure above illustrates roles and example responsibilities of key players in a proposed approach to the provisioning of combat information management. In that proposed approach, combat information management support ranges from near real-time intelligence to longer-term substantive analysis.

In particular, the panel recommends the creation of three distinct levels. At the first level, closest to the operator in space and time, combat information specialists answer, find answers to, and anticipate questions from commanders and operational users in the field. In

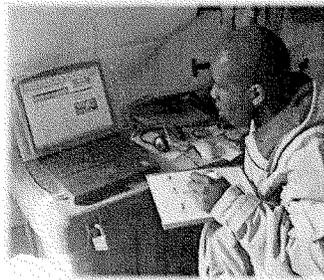
developing answers to those questions, they may collaborate with combat information specialists supporting other units and commanders and/or they may work with knowledge managers who identify, discover, extract, organize, catalog, and maintain information about a selected set of topics. Knowledge managers, and others, utilize subject matter experts who provide in-depth knowledge, advice, and consultation in highly specialized areas.

Effective combat information management will require further refinement of roles and responsibilities, as discussed below. It will require development of concepts of operations and staffing plans. It should build on current service and combatant command efforts in this direction as well as intelligence community assets. Success will require dedicated and trained staff at multiple echelons, although in many cases this will be possible through the redefinition of existing staff. A primary result will be seamless, persistent, expert information support as units rotate in and out of the theater.

While it is clear that advanced information discovery technology will support these specialists, a primary finding is that technology alone will not solve the problem. Several existing technologies can support each of these roles. This can include wikis, blogs, and collaboration tools (see: http://en.wikipedia.org/wiki/Military_Occupational_Specialty). In fact, the Air Force has defined an Information Manager specialty (<http://usmilitary.about.com/od/airforceenlistedjobs/a/afjob3a0x1.htm>).

Combat Information Specialist

- Anticipate and track operational information needs
- Extensive network of contacts for information and intelligence
- Answer operational requests
- Disseminate to combatants and share with peers
- Provide knowledge managers with after-action reviews
- Integrated into units at all echelons
- Have access to classified information at SECRET level



Combat information specialists answer operational requests, anticipate and track operational information needs, and disseminate critical information to combatants—both in mission rehearsal and preparation and in real-time support of mission execution. They are integrated into units at all echelons and have an intimate understanding of the unit's missions and objectives. As such, they are essential elements of the unit fighting team. They have access to classified information typically at the SECRET level, and possess an extensive network of contacts for information and intelligence. They share information with peers in the combat theater, can act as information liaisons with coalition forces, and provide knowledge managers with assessments of the value of information, as well as after-action reviews that knowledge managers assimilate into their individual domains as appropriate.

Knowledge Manager

- Obtain, organize, maintain, and share operational and technical knowledge
- Know sources of expertise and intelligence, extensive network of expert contacts
- Arbiters of quality
- Aware of operational concerns and discover operational insights
- Knowledge manager services shared across units, dozens initially
- Examples: improvised explosive devices, surface-to-air missiles, Islamic culture, economics, political, ...
- Not necessarily subject matter experts

Knowledge managers are responsible for obtaining, organizing, maintaining, and sharing operational and technical knowledge in a specific area of focus. For example, there might be knowledge managers focused on improvised explosive devices, surface to air missiles, Islamic culture, regional economics, or regional politics. While they are not necessarily subject matter experts, they need to have knowledge of the best sources of information and possess an extensive network of expert contacts. While there is no need to physically be collocated with operators, they are intimately aware of operational concerns and discover operational insights via their interactions with combat information specialists and operators. One key role they play is as arbiters of quality. Services provided by knowledge managers are shared across units, with dozens initially deployed, growing to thousands at steady state, dynamically altering according to changing information needs.

Subject Matter Expert

- In-depth, long-term professional in a field of specialization
- Perform detailed studies and analyses of specific domains
- On call to advise knowledge manager, combat information specialist, or users as needed
- Examples: university professors, national laboratory scientists and engineers, military specialists

Subject matter experts possess in-depth, long-term professional knowledge in a field of specialization. They perform detailed studies and analyses of specific domains (such as improvised explosive devices, surface to air missiles, Islamic culture). They are on call to advise the knowledge managers, combat information specialists, or users as needed. They may come from any sector, including university professors, national laboratory scientists and engineers, and military specialists. An essential enabling service will be the maintenance of a database of experts that can be semi-automatically generated using commercial tools (such as Tacit.com or AskMe.com).

Combat Information Capability Includes Enhanced Command and Control Capabilities

- Commanders need to understand, command and control, operate, defend, and attack in cyber space at the operational level
 - During combat operations adversaries will attempt to penetrate or disrupt combat information capabilities
 - Commanders need to monitor and respond to adversary's actions
 - Combat planning must include contingency plans for cyber space actions
 - Operational level commanders will need cyber space forces capable of conducting and supporting combat operations
- Services need to organize, train, and equip cyber forces
 - Develop technological and procedural capability
 - Exercise as part of operational force exercises
- Combatant commanders need planning staff expertise to develop combat information planning annexes

Today, commanders take the command and control of a functional area of combat capability as a given. In terms of combat information, they manage their command and control staff to get the right information in the right form at the right time. To fully realize the potential of network-centric operation, commanders need to take control of their information and the associated infrastructure (the CIC). This ultimately involves two major elements. First, the commander needs to recognize that this is one of the critical tasks. Second, the commander will need the staff, tools, and processes to gain situational awareness of the CIC.

As much as a fully capable information system is needed throughout a mission, adversaries are well aware of U.S. dependence on that capability, and have capabilities of their own to disrupt the CIC in a variety of ways. U.S. actions may also disrupt the capability. The commander must be able to maintain current situational awareness of the CIC and be able to relate the current status to mission capability. The

commander must also be aware of enemy efforts to disrupt operations, so that an attack can be anticipated and countered with a response.

As the commander and his or her staff develop mission plans, contingency plans are necessary for degraded operations. The degradation could be in a variety of areas, such as bandwidth, latency, corrupt data, coverage, or protection. Sometimes, contingency planning may result in a different operating approach to offset adversaries' actions.

A CIC offers both a challenge and an opportunity. The challenge is stated above. The opportunity is to take a giant step forward by integrating additional CIC into the overall command and control function. Commanders need to be able to have command and control of critical information. This will bring together both kinetic and non-kinetic attack elements into a unified system and as a step toward providing a unified approach to the world of the cyber command and control, which historically has been treated in separate systems. This unification of command and control processes will allow commanders to have a tool set that manages cyber actions and also allows management of the CIC to support other attack actions.

Specifically, an intellectual foundation is essential for developing future combat information concepts, educating commanders on the art of combat information dominance, and directing commanders to develop concepts of operation and contingency plans for operating with degraded networks.

In order to make this a reality, each service will need to organize, train, and equip cyber forces. This will need to address more than just the network. It must also include the information management functions that have been discussed in this report. New tools and processes need to be developed for each of the three major information management staff positions: combat information specialist, knowledge manager, and subject matter expert. These staff elements will need to be trained on the tools and procedures. This training will need to extend to exercises such as division mission rehearsal exercises, where command and control of the CIC is exercised along with other joint warfighting capabilities.

Finally, information management staff expertise should be leveraged to develop a new combat information planning annex. Similar to other planning annexes such as logistics, the mission plans will address all of the issues with deploying, operating, and defending a CIC in support of operational mission.

ISR is an Essential Part of Combat Information Capability

- Most of the warfighters' dynamic information is provided by ISR sensors
 - Delayed or denied access to ISR data impacts operational effectiveness
 - Lack of knowledge of planned ISR capability limits integration into the operations tempo
- Recognize the value of treating all space-based, airborne-manned and unmanned systems, and ground sensors as elements of a single system
 - Establish a single sensor management approach
 - Network-enable all ISR data and metadata to ensure availability for the warfighter

The warfighter is dependent on ISR sensors for most dynamic combat information. While some part of sensor data is usable only when analyzed, much of the reconnaissance data requires immediate access because of the time-critical nature of combat operations. Thus, limiting access to ISR information has a significant impact on combat operations. Currently, combat information requirements compete with national intelligence needs for space asset coverage. The uncertainty of satellite coverage causes operational commanders to rely more on theater-controlled assets to ensure coverage, usually to the detriment of lower priority requirements. The lack of knowledge of planned national ISR limits the ability of commanders to integrate ISR into their operations tempo at all levels and sub-optimizes a limited resource.

Thus, the department needs to recognize the value of treating all space-based, airborne-manned and unmanned systems, and ground and maritime sensors as elements of a single system. Ground combat units are acquiring hundreds of unmanned aerial vehicles with improving

sensors. Ground sensors are becoming more effective. All these systems can be more valuable when the data is integrated with other sensor data. The key is to network-enable all ISR data and its metadata to ensure timely availability to the warfighter.

This capability, when fully implemented, will reduce lead times for dynamic tasking of sensors, thereby greatly reducing the time to respond to time-critical targets.

Recommendations for Combat Information Capability

- Create a Combat Information Capability (Deputy Secretary of Defense)
 - Prepare commanders to execute command and control of their Combat Information Capabilities
 - Create a Defense Readiness Review System category for Combat Information Capability readiness
 - Create a system to manage combat information
 - Include combat information support staff, combat information specialist, as well as knowledge manager and subject matter experts
 - Provide commanders at 3 and 4 star level with combat information integrator officers on their personal staffs
 - Provides combat information management training and capabilities
 - Develop / acquire tools and develop TTPs for commanding this system of systems
 - Develop dynamic, integrated ISR capabilities (Commander, U.S. Strategic Command)
 - Provide operational commanders with space platform tasking visibility as a basis for planning theatre assets
 - Plan ground segment improvements to provide more dynamic tasking with reduced lead times
 - Implement policy changes that permit declassification of sensor data to coalition partners, other government agencies and non-government organizations

The panel recommends the Deputy Secretary of Defense direct creation of, and allocate resources for, a Combat Information Capability across the department, since all military commanders must undertake new ways to execute command and control of their combat information resources and capabilities. In order to maintain oversight, the panel recommends that these new capabilities be monitored by creating a Defense Readiness Review System category for CIC readiness. In addition, Joint Forces Command needs to prepare commanders to effectively command and control this capability.

A CIC must contain the following capabilities:

- It must include execution elements of a combat information support staff: combat information specialists, knowledge managers, and subject matter experts.
- The CIC must include robust combat information management training and education, and the capabilities to support such activity.

- The CIC must acquire the proper tools and develop tactics, techniques, and procedures (TTP) for commanding this new capability.
- The CIC must deliver dynamic, integrated ISR capabilities, which will provide operational commanders with visibility of the tasking of sensors and then allow the commanders to effectively plan theater assets.

Chapter 5. Tactical Operations

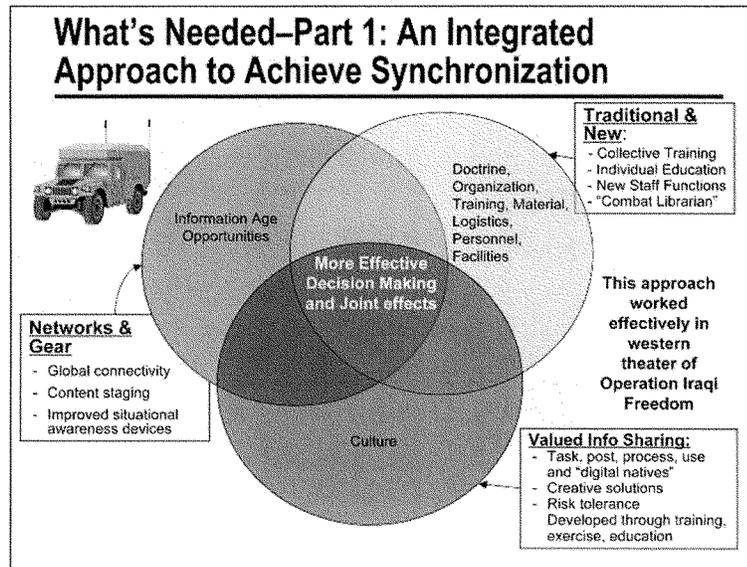
Why are tactical operations different?

- Challenges of ensuring robust, redundant communications, and information availability across the “last tactical mile”
- Historic challenges in accurate, timely bi-directional information flow and synchronization of combat power solving these requires enhanced networks and data, as well as doctrinal and TTP changes, focused training, and a culture of information sharing.

The domains of warfare have been defined as physical, informational, cognitive, and social. The distinctions between and interaction of each domain are generally consistent down to the tactical edge. A generally held belief for net-centric proponents is that solving the “last-tactical mile” communications challenges completes the promise of net-centric capabilities. While better communications at the tactical level closes the gap between the promise of net-centric operations and the state of the art, it is not enough.

Improving net-centric operations in the cognitive and social domains is the area that, in addition to better communications, will begin to close the performance-promise gap. Notwithstanding the current array of physical and informational challenges in net-centric operations at all levels, most practitioners operate in a nearly homogeneous command and control environment. Headquarters staffs

with varying degrees of net-centric capabilities are managing information, facilitating decisions, and communicating to other staffs or platforms. It is at the tactical level that the Clausewitz warning “everything is very simple in war, but the simplest thing is difficult” is most pronounced.



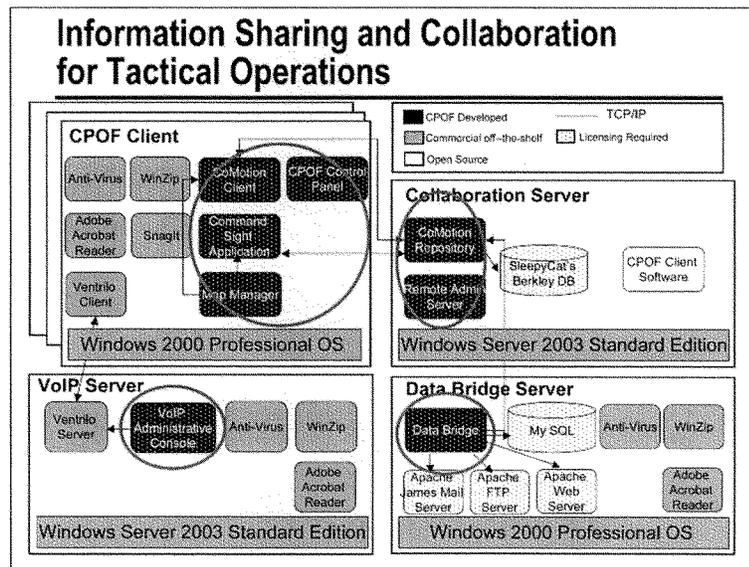
The true success of information management in net-centric operations depends on the successful integration of technology across disparate systems combined with the willingness of organizations to gain experience and adapt both culturally and organizationally.

An excellent example of this combination is reflected in operations in the western theater in Operation Iraqi Freedom. In what was arguably the most networked battlespace in history, commanders created combat power through network-centric systems, doctrine, organization, training, materiel, logistics, personnel, and facilities, and organizational culture.

During Operation Iraqi Freedom Phase One, coalition forces in the western theater accomplished all of their assigned missions, including prevention of all Scud launches, while operating at a 500:1 ground-force disadvantage. The integration of existing command and control systems allowed more rapid response (nine minute response times) to time-

sensitive targets while avoiding *any* air-to-ground fratricide during hundreds of engagements.

MITRE conducted a detailed study of these operations including in-depth interviews with warfighters throughout the kill and command and control chains. This study led to further investigation of particular systems, associated TTPs, and organizations. MITRE concluded that the loose coupling of networks that provided situational awareness from ground-to-air and air-to-ground enabled the coordination necessary to support lightly equipped ground forces. This enhanced communications infrastructure and collaborative tools enabled robust command and control networking that expanded both reach and richness of the information. The MITRE case study demonstrates that successful combat integration and decision-making depends not only on the successful integration of technology across disparate systems but also the vital importance of an organization being adaptive both culturally and organizationally.



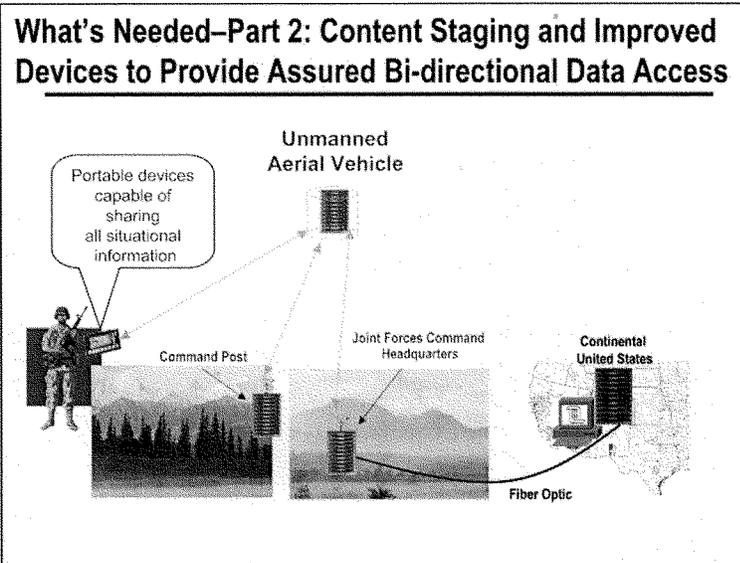
A critical aspect of successful military missions is having a deep, shared understanding of the current situation and the mission objectives, not simply to have a plan. One of President Eisenhower's quotes captures this quite well, "In preparing for battle I have always found that plans are useless, but planning is indispensable." One way, and perhaps the only way, to achieve this deep, shared understanding is to provide the team with a collaborative visualization environment that allows team members to capture their understanding of the situation, share it with others, and collaboratively develop plans to achieve mission objectives.

This is how Command Post of the Future is being used by forces in Iraq today. Distributed, collaborative planning became popular in the early 1990s when networks and video teleconferences were becoming available at the higher echelons. What is different today is the fact that

with systems like CPOF, rather than dedicating bandwidth to share a picture of someone's face, the bandwidth is being used to share thoughts, and thus supporting true collaboration, rather than simply distributed planning. Since the focus is on sharing data, and doing so in a bandwidth efficient manner, CPOF has demonstrated the need and high value of information sharing and collaboration at the tactical levels.

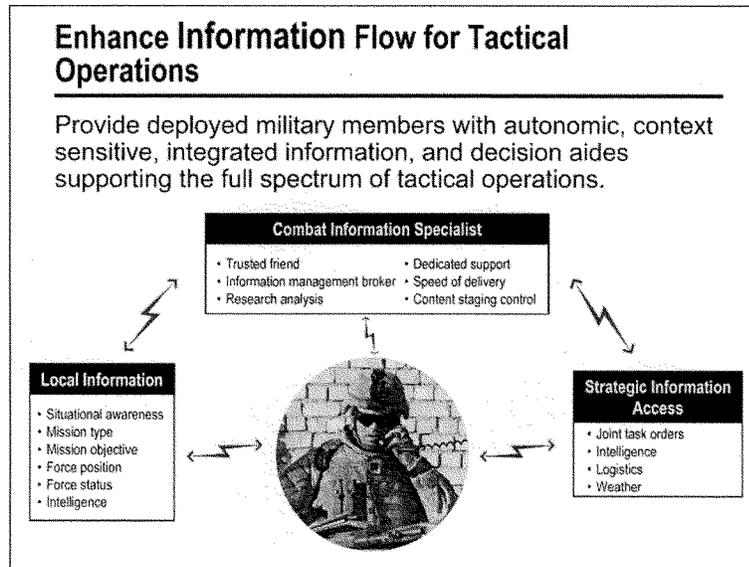
An interesting perspective is how this capability was developed. The CPOF system is built on three core commercial products. One is the database system, which in this case is Berkeley DB, a very popular and powerful database system now owned by Oracle (owned by Sleepy Cat Software when CPOF was first developed). Another commercial component is the 3D visualization package called 3DJava, a high performance tool set developed by Oculus Software. The final commercial component is a collaboration and visualization environment called CoMotion, originally developed by Maya Viz.

Working closely with users, the developers from Oculus and Maya, as well as other small companies, discovered ways that users wanted to use this collaborative, visualization capability. Those same developers then tailored, augmented, and extended the core commercial products to provide military capability. Initially this was done in the context of a tactical user, but without full understanding of the issues of the tactical environment. Once the system was deployed, other modifications were made to deal with the disadvantaged communications, which had frequent drop outs, high packet loss, and high latency. This experience demonstrates that commercial technology can be adopted and successfully adapted to military use.



The CIC described in this report will constantly be subject to attack by an adversary, both via non-lethal and lethal means. Therefore, the system-of-systems must be capable of degrading gracefully when attacked. Currently most combat data and information content is stored in data storage repositories far to the rear and/or in the continental United States. From the commanders' perspective, this creates a huge vulnerability that may lead to catastrophic failure of their command and control information systems in the event of an attack on various communications systems and nodes.

In order to greatly reduce the vulnerability of the CIC to attack, the panel determined that critical battlefield information should be staged in the area of responsibility and/or perhaps even stored in an unmanned aerial vehicle over the area of operations and within direct line of sight of sensors and ground forces. This operational concept is depicted in the figure above. In essence, critical battlefield data would be well protected (firewalled) and staged forward in several servers distributed throughout both the forward and rear areas. Such architecture would not only provide a means to isolate and secure various data sources against an



The tactical warfighter can clearly benefit from improved access to time-sensitive information and decision aids. The challenge is how to provide that information given the communication and time constraints of the tactical environment. The solution involves three key components. First is the combat information specialist, who can ensure that the warfighter will get the information needed in the right context. Second is a prepared set of information that comes from the local environment, and is very specific to the mission at hand. This information will be staged forward so that the warfighter will have access to it even if there are communication outages. Third is the reach-back to more strategic information assets and general reference information. Due to the harsh nature of the tactical environment, these three components need to be able to provide value to the warfighter separately, but combined will provide a complete capability to access the full range of information required for tactical operations.

The need, then, is to provide a device that the warfighter can use to access this information.

adversary's attack, but it would also allow data to be replicated between data sources whenever available bandwidth allows. Staging content in theater would not only reduce system vulnerability to attack, but it would also potentially reduce information query response times. Thus, the advantages to all would be reduced system vulnerability to attack, better use of available bandwidth for data transfers, and greatly reduced query response times for warfighters.

Warfighter's Combat Information Portal



Commercial Game Device



Commercial Phone /
Personal Digital Assistant

Example Devices

- **Required Capabilities**
 - Voice and data communication
 - Including imagery and video
 - Collaboration
 - Capture situation reports
 - Access key status elements
 - Stage key mission information
 - Queue outgoing communications
- **Device Characteristics**
 - Low power
 - High resolution display
 - Operates in wide variety of light conditions
 - Rugged
 - Sufficient storage for staging content and queuing communication
 - Simple, intuitive interface

Providing combat information to the edge will require innovative devices that will be low power, rugged, operate in a variety of climactic conditions, integrate voice and data communication, and essentially serve as the single portal to the tactical fighter for combat information, communication, and collaboration. This device needs to address the realities of the tactical environment, and thus be simple and intuitive to operate.

This portal device could potentially be derived from commercial technology. Cell phones, PDAs, and portable game devices should all be explored as candidates to meet this important operational need.

The operational device should provide warfighters the following capabilities:

- voice and data communication with the core mission team as well as other entities, such as a combat information specialist, joint forces, coalition forces, or non-government organizations

- collaboration in support of situational awareness, planning, mission rehearsal, and execution
- situation reports such as SALUTE reports
- blue force positional information
- access key status elements such as CIC and network status
- stage key mission information locally, as well as queue key communications when the network is down

For this device to be practical, it will need to have the following characteristics:

- low power
- operate in a wide variety of lighting conditions without compromising a combatant's position
- rugged to withstand the rigors of combat
- sufficient storage for staging content and queuing communications

Commercial capability can be easily and economically adapted to meet this requirement. The objective is to have these devices so inexpensive that newer generations of technology can be quickly fielded to maintain the tactical advantage and avoid technical exploitation by an adversary.

Recommendations for Improving Information Flow to and from Tactical Commanders to Enable Decision-making

- Introduce the concept of into the GIG architecture in an effort to protect the network against communications failures or attack (ASD/NII)
- Focus additional resources on fielding improved voice and data systems at the tactical level (ASD/NII)
- Provide commanders with rigorous, focused training on the art and science of combat operations integration and information / network management (CJCS)
- Formalize the requirement for an “exercise and training network” linking all echelons (CJCS)
- Adopt a doctrinal joint staff function for combat information management (CJCS)
- Adopt a doctrinal “combat librarian” global reach capability for tactical commanders (CJCS)

The operations panel reinforces the view that cultural characteristics occasionally prevented realization of net-centric operations tenets. A net-centric culture revolves around the belief that the information one element produces may be useful to another element for unforeseen reasons. Thus, the information solution that enables better decision-making is based on the faith that information made available to the enterprise will increase combat power in unspecified forces. Decision makers must turn from the “hunt” for combat power toward the “farming” of combat effects through better combat information management processes like the use of combat information specialists. This cultural change requires leaders and soldiers to take risks in developing new solutions, and an organization that tolerates individuals willing to take risks.

The following recommendations are needed to improve the ability of commanders at all levels to make decisions and win:

- First, develop a forward content staging base to enable bandwidth-disadvantaged tactical users timely access to information posted by individuals from across the enterprise.
- Second, provide warfighters—particularly at the last tactical mile—technologically better tools (e.g., the Joint Relay Extension and Battle Universal Gateway Extension at the unit level, and soldier handheld devices operating on the soldier radio waveform) to help them access, share, and manage information.
- Third, improve command and control by implementing a tough, rigorous training system for commanders and units on the best ways to employ and manage combat information capability.
- Finally, create a focused staff function and organic combat information specialist, to enable both soldiers and commanders to optimize information management and make the best possible decisions.

Chapter 6. A CIC is a Critical Defense Weapon System

A Combat Information Capability IS a Critical Defense Weapon System

- A modified approach for providing information to and from the tactical level assumes that
 - Modern technology links together the entire battle space
 - Every military platform and person in the battle space is a sensor and node on the network
 - Global, interoperable net-centric operations will increase combat effectiveness
- A combat information capability must therefore be managed and protected as effectively as any critical defense weapon system.
 - This capability will be an enormous operational differentiator and will provide the nation with an unprecedented capability to manage its assets in the time of conflict.
- Information management systems are managed more as a technology asset and curiosity than a critical defense weapon system.

As discussed in the preceding pages, tactical operations require enhanced networks and data, as well as doctrinal and TTP changes; rigorously, focused training; and a culture of information sharing. This culture assumes that:

- Modern technology links together the entire battlespace, from the strategic to the tactical.
- Every military platform and person in the battlespace is a sensor and node on the network.
- Global, interoperable net-centric operations will increase the combat effectiveness of U.S. military forces.

The preceding section illustrated the power of staging critical combat information forward, a combat information specialist, and doctrinal joint staff functions for combat information management for the tactical commander. Because these attributes of the CIC are so critical to the current and future success of U.S. forces, it is imperative that the CIC is treated not as a force enabler or a mere staff function, but instead as a critical defense weapons system. This capability will be an enormous operational differentiator for U.S. forces and will provide the nation with an unprecedented capability to manage its assets during combat, stabilization and reconstruction, and peacetime contingencies.

The implications of treating this CIC as a critical defense weapon system are significant.

Treating Combat Information Capability as a Defense Weapon System

- Fielding and operating a Combat Information Capability requires, for example:
 - Commanders that are trained and empowered
 - Effective leader development
 - Robust training and exercises
 - The ability to operating effectively with military and non-military partners
 - Equipment and tools
 - System operational management
 - Innovative governance and acquisition
 - A review process to assess progress and adjust trajectory

Commanders need to have the responsibility and authority that allow them to take control of both their information and the associated infrastructure. Only after commanders are empowered can they move forward with developing the tools and processes to control this critical capability. In addition to empowering commanders, there is a need to develop effective leaders that can lead in a net-centric environment. A net-centric leader must do more than simply be knowledgeable about information systems technology. They need to be information age leaders—that is, they need to understand all aspects of how information can be used to provide their forces a competitive advantage. One of the interesting aspects of unleashing information in an organization is that it will have the effect of flattening the organization, thus enabling a more rapid and effective collaboration.

Effective and robust training is essential to this critical weapon system. The training cannot simply be to a fixed set of processes, but instead needs to focus on the principles of information management that will support flexible processes. This training needs to be connected

with realistic exercises; therefore this is not simply an academic activity but one that will prepare the warfighters for combat.

In addition to preparing personnel, another aspect of a critical weapon system is the operation of that system. One very important aspect of the operation is ability to interact with other systems and other, non-DOD participants. This includes coalition partners, other government agencies, and non-government organizations. This will certainly require technology to enable information sharing, but it will also require procedures to guide users through the process of sharing information with people you might not ordinarily trust.

Another element of this critical weapon system is the identification and development of the set of the tools necessary for daily operation. This includes tools such as a help desk to support a wide range of users, tools for backup and restoration of the database, and network diagnostics. The combination of these tools, with staff and procedures, will complete the system operational management.

Part of the day-to-day management of the system is the collection of new requirements that emerge from innovative uses of the tools. Many of these requirements can be satisfied with the development of new techniques and procedures, but others may require developmental activities as well. To be able to deal with both the emergent and new development requirements, an innovative governance and acquisition process will be essential to allow the CIC to keep pace with commercial technology.

Finally, in addition to a day-to-day systems management process, a longer term review process to assess progress and adjust trajectory needs to be put in place. One thing that would facilitate this and other processes is the right instrumentation to provide analysts with the opportunity to understand how the system is being used and determine the impediments to reaching its full potential.

Implications for Commanders

- **Operating with degraded networks**
 - Develop concepts of operations and contingency plans, exercised regularly, that deal with denial-of-service attacks, network penetrations, and other degradations
 - Must have necessary network status information to make risk-managed decisions about mode of operation
- **Embracing redundancy**
 - Assume a hostile environment with an adversary actively trying to deny access to our capabilities, not to mention the natural friction with any technology (Murphy's laws).
 - We need to have more than one way to satisfy an objective
 - Redundant caches of information and communication paths

For the tactical commander, operating with degraded systems (weapons, communications, logistics, maneuver) is the norm, not an anomaly. It is this defining quality of the tactical environment that requires modifications to the current deployment of net-centric capabilities. Any solution to challenges at the tactical level must start with the nature of the tactical environment, not the nature of the technical challenge. Two significant concerns voiced by tactical commanders regarding the ability to leverage the power of information are redundancy and robustness.

The redundancy of the network and the critical data on the network is a key attribute given the immediacy of enemy actions, the environment, and even unintentional errors. A practical knowledge of how the various networks work together and what options exist to restore or work around failures are key requirements for commanders in a net-centric battlefield.

Implications for Commanders (continued)

- **Ensuring robustness**
 - Because our adversaries will likely push us in unanticipated ways, our systems will need to be able to operate in modes that accommodate
 - Greater scale of users
 - Higher bandwidth of sensor data, collaboration traffic
 - Communications links with less than ideal performance characteristics
 - Designed for graceful degradation with feedback to users to reflect current system performance
- **Must be provided necessary network status information to make risk-managed decisions about mode of operation**
 - Available capacity, estimated extent of penetration

Robustness of the information system is required for more than the obvious redundancy implied in the engineering sense of the term. A system that is robust will empower tactical commanders by instilling confidence that the information systems are every bit as capable as other tactical capabilities.

Implications for Leader Development

- **Leverage non-military “networking culture”**
 - Civilian expectations for information access and collaboration is empowering local adaptation (cell phone web access, myspace.com, etc.)
 - Emergent skill sets are ahead of organizational design—knowledge brokers, human web-crawlers, etc.
- **Focus education on net-centric operations “application” not technical theory**
 - The art of net-centric operations is not keeping pace with the science
 - Case studies of net-centric operations, using contemporary operations and civilian applications
- **If leader development lags technical development**
 - A decrease in the power of a combat information capability; confidence grows from technical and tactical proficiency.
 - Increased risk to and from the network; risk management requires confident decision makers who can adapt to the challenge of degraded network operations.

Tactical leaders must learn to leverage a nonmilitary “networking culture” to accelerate tactical applications of information networks.

A long standing truism is that all war takes on the attributes of its age. To the extent that this statement is true, network-centric is more a description of the condition of age than it is an operational concept. In the frenzy to develop and deploy information networks it is easy to lose sight of the fact that humans have always created and expanded social and physical networks. The recent phenomenon of creating and expanding into the information domain is a logical progression. The resulting culture² is a determining factor of how military operations are organized, as much if not more than any forward-leaning doctrine. The cultural drivers of the military application of networks are uniquely civilian.

2. Culture is defined as “The system of shared beliefs, values, customs, behaviors, and artifacts that the members of society use to cope with their world and with one another, and that are transmitted from generation to generation through learning.”

Leveraging the civilian “networking culture” means recognizing solutions that come up from the bottom (the edge) of the system. Solutions applicable to the tactical battlefield are being discovered by the tactical practitioners who are conditioned, in many cases, to solve information challenges in their civilian lives.

The CIC must focus education on net-centric “application,” not technical theory. The art of war and the science of war have always been an interactive dynamic. They are two sides of the same coin and often used interchangeably. As net-centric operations have matured into a real, albeit not fully realized or understood capability, the relationship between the science (technology) and the art (commander’s realized intent) has become unbalanced. Bringing the world of commercially driven hardware and software into the realm of military operations is occurring at a dizzying pace and is obscuring the distinction. In fact, many of the most virulent critiques of the role and potential of networks in warfare are railing against the tendency to let the science of war overwhelm the art.

The current generation of U.S. military personnel could arguably be counted as the most experienced cohort in the nation’s history. The number and variety of military operations during the past 20 years range across all but the highest end of the spectrum of conflict. During this same period of time the impact of information systems and networks on tactical military operations began to play a more dominant role. The tacit knowledge of the current cohort in the application of information networks to the problems of warfare is a national asset. This same generation is living with the exponential changes in the civilian world. It is the combination of living with the most leading-edge and fungible technologies in the civilian world and their operational experiences (good and bad) that makes bottom-up case studies so critical to institutionalizing net-centric operations.

The implications for leader development are critical. There is a cost to allowing combat leaders and network developers to evolve on parallel but divergent paths. Combat leaders need to be trained on net-centric processes and technologies, while network developers need to better understand the challenges of conducting operations in a net-centric environment.

Well-trained and creative leaders can adapt to the challenge of degraded network operations. Operational risk management is a creative, not technical, process.

Implications for Training and Exercises

- **Educate**
 - Develop an intellectual foundation for future combat information concepts and then create courses to educate the entire force on these core concepts
 - Commanders need to be educated on the art of combat information dominance
- **Train**
 - Using data and lessons captured from current combat missions
 - With new information templates, organizations, capabilities, concepts of operations
 - Distributed, home station training opportunities
- **Experiment**
 - Campaigns of experiments allow full exploration of ideas
 - Explore interplay between technology and concepts of operations
 - Challenge competition maximizes pace of discovery and depth of exploration
 - Unfettered and highly skilled adversary; no cultural limitations; physics only restrictions
 - Capture, archive, and mine experiment results to develop insights
- **Exercise**
 - Non-scripted, unfettered adversary, fog and friction
 - At different scales
 - Focus on exercising decisions

To realize the full potential of network-centric operations, a full training and education system will need to be established. The first order of business is to develop the intellectual foundation of combat information management. This foundation will become the basis for enhancing and extending the core capabilities, and will also provide commanders the basic tools needed to flourish in this new era to achieve information dominance over the adversary. Once commanders have the freedom to “maneuver” in information space, additional advantages over the adversary will become apparent.

A key component of any major weapons system is the training program. An effective training program will take the results of the education program and make it intuitive. It is important to train with information that is close to what commanders will deal with in combat. The CIC should be developed to allow easy capture of information to support training programs. One aspect of the training should include the ability to develop new information templates on the fly, as well as enabling new organizations and concepts of operations. By including these aspects in the training program, the warfighters will be able to

tune their CIC in combat. The CIC is naturally distributed, providing an opportunity to leverage home station training. The result is the ability to deliver more training at a drastically lower cost.

An important aspect of the CIC is that it will always be evolving. The experience with CPOF has shown that users will develop new information templates and new procedures in order to quickly tune the CIC to the situation at hand. There is a great opportunity to build facilities into this weapon system to allow for continuous experimentation, to maintain dominance in the information domain. Much of the experimentation will explore evolutionary extensions to the capability, but there also needs to be some experimentation devoted to more revolutionary ideas.

To get the most out of experimentation, it should be conducted in a challenge-competitive environment, with unfettered adversaries. Such an approach will ultimately prepare commanders and staff to deal with a degraded CIC capability, and allow them to develop intuition on the elements of the system they can count on. This experimentation process will tune new capabilities that should greatly enhance the core capabilities. Many of the experiments performed may not provide the immediate answers but, over time, a series of experiments should provide users, developers, and technologists key insights into where the high value capabilities are. Many of these experiments can take place in both the training and exercise venues.

The final piece of the training and education element of this critical weapon system is the exercise. Commanders need to be given the time and resources to exercise staff and forces, in as realistic environment as possible. The CIC needs to be exercised at every echelon, and at each level, and the focus needs to be on using the information for making decisions. Decision exercises are a very effective means for bringing education and training together.

Implications for Operating Effectively with Partners

Partners span the U.S. Government...

Intelligence community
 Department of State and USAID
 Departments of Treasury and Justice
 Dept. of Homeland Security (including FEMA)
 State and local governments

...and beyond

Allies: United Kingdom, Australia, Japan, etc.
Coalition partners: India, Pakistan, Indonesia, etc.
International organizations: NATO, United Nations, Red Cross, etc.
Non-government organizations: CARE, Mercy Corps, etc.

- Current and future contingencies require the integration of all elements of national, and often international, power
- Common command and control system is key to interoperability with allies and coalition partners
 - CENTRIXS is current solution for this challenge but has its limits
 - CENTRIXS does not address info sharing with non-military partners
- Release of and sharing information with non-U.S. military sources has been problematic in every recent contingency; must institutionalize ability to
 - Plan and operate with allies and coalition partners
 - Timely and effectively share unclassified information with appropriate organizations
- Policy and process solutions are as important as technical solutions

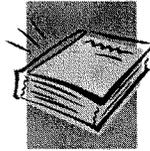
One of the defining aspects of today's military environment is that the United States has moved well beyond joint operations. Today's operations are fully integrated with key interagency, state and local government, alliance, coalition, host nation, international, and non-governmental organizations and actors. Each of these actors generally operates on its own distinct network, although sustained operations during the past decade in the Balkans and now in Iraq and Afghanistan have led to the development of tools and arrangements for information sharing and collaboration. These efforts, however, have often been ad hoc and have not allowed for the true integration of all elements of national and international power.

Because future contingencies will almost certainly require collaboration of U.S. forces with interagency, coalition, and non-governmental actors, DOD must work to improve and institutionalize its ability to work effectively with partners in all stages of combat, stabilization, and reconstruction. CENTRIXS, for example, has been the vehicle for collaboration between U.S. and coalition forces during Operations Enduring Freedom and Iraqi Freedom. CENTRIXS has

been successful in many ways, but it is limited. It does address information sharing with non-military partners, because it will not allow for U.S. and coalition forces to plan and operate on the same network. Although it is vital for operational security reasons that U.S. forces maintain this firewall between U.S. military networks and the networks of coalition (with the partial exception of the United Kingdom and Australia) and non-military partners, it is equally vital that the department work to find ways to improve the current situation in this area. Technical solutions will be helpful in this regard, but policy and process solutions are likely to be of equal or greater importance.

A Combat Information Capability Strategic Plan

- A strategic plan to guide the development of a combat information capability
 - This plan should
 - Identify required resources
 - Establish a timeline and identify key milestones for plan implementation
- This plan must address the major actions required to develop a combat information capability:
 - Train commanders to effectively utilize information management infrastructure
 - Concepts for information organization and access
 - Doctrine for combat information capabilities
 - Education and training programs including information management
 - Command and control of combat information capabilities
 - Education in the art of combat information dominance
 - Exercises and experiments for realistic operational scenarios
 - Research on advanced information concepts
 - Lessons learned from current operations



The best way to articulate and develop a CIC across DOD is to create a strategic plan drafted under the authority of the Chairman of the Joint Chiefs of Staff (CJCS). This plan must address the major actions required to develop a true CIC, including:

- concepts for information organization and access
- doctrine for combat information capabilities
- education and training programs including information management
- training for commanders to effectively utilize combat information management infrastructure
- command and control of combat information capabilities
- education in the art of combat information dominance
- exercises and experiments for realistic operational scenarios
- research on advanced information concepts
- lessons learned from current operations

This plan also should

- identify required resources
- establish a timeline for key actions
- identify key milestones for plan implementation

Chapter 7. Major Recommendations

Operations Panel Major Recommendations

- Develop a Strategic Plan for a Combat Information Capability (CJCS), including
 - The ability of commanders to command and control combat information capabilities
 - Additional staff capabilities to deal with combat information management, i.e., focused staff, combat information specialist, etc.
 - Experimentation, training, and exercise
- Introduce the concept of “content staging” into the GIG architecture (ASD/NII)
- Continue to pursue solutions that will facilitate automated information sharing with coalition partners, non-government organizations, and first responders (ASD/NII)
- Develop a joint requirement for dynamic, integrated command and control of ISR assets (CJCS)
 - Incorporate the need for space platform visibility tools and ground segment improvements into this requirement (Commander, U.S. Strategic Command)

Field and Operate the Combat Information Capability as a Critical Defense “Weapon” System (Secretary of Defense)

The most significant recommendation of the panel is for the Secretary of Defense to recognize the importance of the CIC as an essential combat capability and declare it a critical defense “weapon system.” This recognition means that the essential elements of the CIC will be planned, programmed, and resourced as a weapons system. The assumption is that the GIG and the network operations to the HAIPE will be provided as planned and the weapon system, including support of the warfighter in the theater, will be provided in a single portfolio.

The proposal is similar to the Air Force decision to recognize the Combined Air Operations Center and its extended elements as a weapon system. In doing so, the manning, equipment, training, exercise, research and development, and other elements are programmed,

planned, and resourced. The consequence has been a more combat-ready capability and planned improvements over the period of the future years defense plan.

A significant challenge will be to decide what programs will make up the weapon system elements. Those communications and information management capabilities required in the battlefield should be part of the weapon system. The proposed information management support elements such as combat information specialists, knowledge managers, and subject matter experts should be included, as well as support for the warfighter outside the HAIPE.

This operational focus requires a strategic plan to lay out the required elements and build them into a CIC. The Chairman of the Joint Chiefs of Staff should develop such a plan with the services as the basis for parts of a program element. The development of the capability and the experimentation, education, training, and exercise of the capability should all be part of the plan.

Because so much of the combat information requirement can be satisfied with existing and planned ISR capability, there is a need to develop a joint requirement for dynamic, integrated command and control of ISR assets. This capability can optimize the allocation of all ISR resources and lead to more robust sharing of tactical combat information sharing. An essential part of building this capability is to incorporate the need for space platform visibility tools and ground segment improvements into this requirement.

The fragility of present and planned tactical communications requires the concept of a forward content staging base at the tactical level. As an example, the warfighter will load the combat information device with the most current information for the mission. The updates will flow to the device if connectivity is maintained. If communication is lost, the information is still available to the warfighter. When communication is restored, new information again flows. It also reduces the amount of information that must be accessed over narrow bandwidth.

The need to share information with coalition partners, non-government organizations, and first responders still requires more

effective solutions. The Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) needs to pursue solutions that will facilitate automated information sharing. Manual manipulation delays information, making it ineffective in combat and some emergency response operations.

The bottom line is to field and operate the Combat Information Capability as a critical defense weapon system.

Appendix A. Terms of Reference

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

MAR 15 2006

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT - Terms of Reference - 2006 Summer Study on Information Management for Net-Centric Operations

The United States military steadily transformed during the latter part of the 20th century by an ever increasing reliance on information networks and their ability to provide wider access to information and to support collaboration. Impressive gains in the usability, usefulness and availability of all forms of information have improved the effectiveness of military operations. Our increasing ability to leverage information and networking will be a critical enabling factor in developing better ways to work with others in the USG and with both coalition and non-traditional partners as we, collectively, undertake the challenging missions of the 21st Century.

Today a Company Commander can control a Division's worth of firepower, tagging and tracking systems promise to significantly improve the logistics chain and the improved availability of intelligence information and greater connectivity between sensors and shooters has increased the effectiveness of our forces and enhanced their security. During the past ten years, we have seen the evolution of military missions driven by adaptive adversaries who recognize our increasing dependence on information networks. Going forward, transformation must focus on addressing the stresses imposed by 21st Century mission challenges associated with stabilization and reconstruction operations in urban and unconventional environments and responses to unforeseen events with catastrophic consequences. Information and the ability that networks provide to make this information available to those who need it, as well as the ability for individuals and organizations to collaborate, are the lifeblood of military and civil-military operations. The quality, reliability, availability, timeliness, discoverability, relevance, and security of information and interactions among individuals and organizations across the enterprise (warfighting, with business and intelligence support) will have profound consequences for successful mission execution.

To date the transformation of the DoD enterprise has focused on improved connectivity, interoperability, and information sharing among disparate joint forces and systems. Future challenges and the need to maintain adequate levels of security, integrity, and reliability will place new demands on our information networks, processes and personnel. As new users demand more information and adaptive information sharing, improved knowledge utilization and better tools for information discovery will become critically important. "Googling" and "blogging" are making their way into military operations at all levels, but the full implications of this revolution are as yet unknown and we have no clear direction and defined doctrine.



You are requested to form a Defense Science Board Summer Study assessing the Department's strategy, scope and progress toward achieving a robust and adaptive Net-Centric DoD Enterprise.

The Summer Study should:

- Examine the operational value enabled by networks and networking and their impact on innovations across the Enterprise. Assess the implications of new and innovative approaches to command and control structures, capabilities, and processes, including interagency, coalition, and non-traditional participants, the need for greater adaptability and the emergence of new missions such as counter-insurgency, stabilization and reconstruction operations, counter-WMD, and catastrophic disaster support.
- Evaluate the underlying framework, architecture, processes and organizational structures that are in place or being pursued to deliver the power of information to the DoD enterprise as well as potential external partners. Explore Enterprise Wide cost/risk trades between bandwidth, quality of service, network availability, network security, information integrity, information sharing, and collaboration.
- Assess the state of the art in knowledge utilization. Particular attention should focus on information discovery, sharing in a secured networked environment, visualization and collaboration. How are emerging techniques being incorporated into operations both in the near and far term. How is information being turned into knowledge and then coordinated action as quickly as possible?

The study will be sponsored by me as the Under Secretary of Defense (Acquisition, Technology and Logistics) and the Assistant Secretary of Defense (Networks and Information Integration). Mr. Vincent Vitto and Dr. Ronald Kerber will serve as the Summer Study Task Force Co-Chairmen. Mr. John Mills, OASD (NII), will serve as the Executive Secretary. LTC Scott Dolgoff will serve as the Defense Science Board Secretariat representative.

The Task force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.



Kenneth A. Krieg

Appendix B. Glossary

ASD/NII	Assistant Secretary of Defense for Networks and Information Integration
CIC	combat information capability
CJCS	Chairman, Joint Chiefs of Staff
CPOF	Command Post of the Future
DOD	Department of Defense
DSB	Defense Science Board
FEMA	Federal Emergency Management Agency
GIG	global information grid
HAIPE	High Assurance Internet Protocol Encryptors
ISR	intelligence, surveillance, and reconnaissance
NATO	North Atlantic Treaty Organization
OUSD (P)	Office of the Under Secretary of Defense for Policy
SOF	special operations forces
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UCAV	unmanned combat air vehicle
USAID	United States Agency for International Development

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

JULY 9, 2009

QUESTIONS SUBMITTED BY MR. ANDREWS

Mr. ANDREWS. What incentives does the DoD have to attract and retain quality skilled IT personnel? How do those incentives compare with the private sector?

Mr. HARP. The DoD must compete with the rest of the Federal Government and the private sector for highly skilled talent with the necessary business, technology and acquisition competencies. Many of the skills that DoD has defined as “mission critical” mirror those defined by the private sector. Generally, and not surprising, some of the most highly sought after skills are those that involve information technology/data architecture and information/Cyber Security (IA). Additionally, knowledge of government practices and DoD regulations, and possession of required security clearances, are lucrative commodities.

The DoD has limited incentives targeted to IT personnel, which are described below. Those it does have often provide only a partial solution. The DoD CIO, the newly appointed IT Functional Community Manager for the DoD civilian IT community, has been working to create a comprehensive strategy that can be used universally to support the management of defense IT occupations. The DoD also has the opportunity to use federal-wide authorities such as recruiting, retention, and relocation bonuses and the student loan repayment program. The challenge is the ability to deploy these tools in a strategic manner for maximum benefit. Unlike the military community where recruiting and retention programs are funded and managed centrally, or DoD’s centrally funded Defense Acquisition Workforce Development Fund, almost no DoD IT civilian workforce incentives are managed or funded centrally.

Scholarships

Information Assurance Scholarship Program (IASP). In 2001, with Congressional support, the DoD CIO established the IASP, a cooperative venture with numerous educational institutions to award scholarships to undergraduate and graduate students enrolled in Centers of Academic Excellence in Information Assurance Education. The IASP enables DoD to recruit top students majoring in various disciplines to fill critical IT/Cyber Security (IA) billets and create a continuous pool of skilled IT professionals to meet current and future work requirements. Current IASP issues:

- Funding levels resulted in only 50% of Components’ requested quotas for the 2009–2010 academic years being filled.
- Lack of a specific hiring authority associated with the IASP has created unintended inefficiencies and inequities such as limiting the applicant pool to students who can complete internships, limiting the appointment term of the graduates, or causing individuals to have to compete for hiring to fulfill their service payback. Creating a simplified and easily understood hiring authority for IASP students would greatly smooth the transition of these students to DoD. DoD supports draft IASP direct hire authority legislation contained in H.R. 2647, sec. 1103 which would resolve this issue.

Direct Hire Authority.

Whenever the IT job market demand increases for new skill sets or additional personnel, it is difficult for most DoD Components to respond quickly as the private sector. Most are not adequately funded to provide recruitment and retention incentives, and as a further complication, Components must comply with the long, onerous recruiting process. DoD (and the rest of the Federal Government) has limited direct hire authority for IT personnel which is targeted solely to “select” information security individuals as described below. To be effective, this authority must be granted to address all the IT occupations that support the critical missions of DoD.

Information Assurance (IA) Direct Hire. This authority is limited to those individuals performing managerial information security functions in grades GS–9 and above within the 2210 series. Those individuals comprise a small number of DoD’s full-time civilian Cyber Security (IA) workforce. Not covered under this authority are key individuals performing technical IA functions including systems administra-

tors and network services providers or individuals performing Cyber Security (IA) functions in other occupation series.

The DoD CIO supports the availability of a comprehensive, expedited IT hiring authority such as that afforded to the Acquisition Workforce in the FY09 National Defense Authorization Act, which modified Section 1705 of title 10, United States Code. Such an authority, judiciously implemented through consultation and direction from the Under Secretary of Defense for Personnel and Readiness, would enable DoD to move more quickly to address challenges such as standing up its new Cyber Command, finding replacement personnel for individuals in IT-intensive commands who will not relocate in conjunction with BRAC, addressing insourcing initiatives, or responding to other Component-level hiring issues.

Special Salary Rates.

At DoD, three IT occupations currently have special salary rates for individuals in the general schedule who are not in pay banded salary programs: IT Specialists, Computer Scientists and Computer Engineers. Although the Special Salary Rates (SSR) were originally designed to be greater than locality pay rates, annual increases to the locality pay tables have outstripped increases to the SSR in many locations, causing significant erosion and even discontinuation of IT SSR for many individuals, both within DoD and across the Federal Government. For example, a GS-9, Step 5, IT Management Specialist in Columbus, Ohio, received a \$7,535 salary differential in 2002 due to SSR; that benefit has eroded to \$6,210 in 2009. A GS-11, Step 5, in the Washington metropolitan area received \$4,025 additional in special salary compensation in 2002. That benefit is gone in 2009 as a result of locality pay outstripping the IT SSR.

Reinstatement of a stronger IT special salary rate would largely impact the GS-2210 series (GS-12 and below) as only 34 percent of DoD 2210 population was in a pay-banded compensation plan at the end of FY2008. Significantly smaller numbers of Computer Scientists and Computer Engineers would be impacted as more of these individuals are in pay banded and demonstration projects already established, providing more comparable salary rates with the private sector. The eroding IT SSR impacts some of DoD's most critical IT workers, including systems administrators, applications software personnel, network services providers, and IT project managers, many of whom are also part of the Cyber Security (IA) workforce.

Lifelong Learning. The rate of change in information technology requires robust professional development programs that provide continuous learning opportunities for DoD IT personnel. These include traditional education and training programs at DoD technical schoolhouses and academic institutions such as the Naval Postgraduate School, the Air Force Institute of Technology and the Information Resources Management College at the National Defense University; tuition reimbursement programs; a commercially aligned certification program for the Cyber Security (IA) segment of the IT workforce; and a retention-focused facet of the Information Assurance Scholarship Program. At the Component level, several organizations have implemented internship programs to attract and develop younger talent to the IT workforce as part of their strategic human capital planning. The goal is to grow these programs to ensure that a continuous pool of skilled IT professionals is available to meet DoD's diverse mission critical requirements.

The biggest differences between DoD and the private sector is the emphasis that the private sector places on the need for pay differentials within the IT sector and their greater flexibility to offer necessary targeted incentives. For instance, while DoD and the IT private sector have offered comparable salary increases of 3.5% in the recent past, average salary increases for select IT positions in the private sector, such as Security Analysts (one of the harder IT jobs to fill) have been as high as 7.7%. The average signing bonus for a private sector IT Manager is typically about \$1,000 higher, however, few in DoD actually receive one. For example, only 55, or 3% of new IT Specialists (which include Cyber Security (IA) personnel, IT project managers, enterprise architects and other critical roles), received a recruitment bonus in FY2007 and less than 70 IT Specialists were enrolled in DoD's loan repayment program that year. Approximately 800 IT Specialists (3% of the 28,000 individuals in the 2210 occupational series) received a retention bonus. These low numbers in DoD are also reflective of the low usage of incentives in federal workforce at large. Many federal Chief Human Capital Officers, when surveyed, have cited lack of funding as hampering their ability to use incentive programs.

Both DoD and the private sector value IT certification programs which have been shown to be particularly attractive to employees under age 35, a key demographic to fill behind retiring baby boomers. If DoD can gain momentum in certifying its Cyber Security (IA) workforce, this is a significant area where DoD may gain traction in attracting and retaining mission critical employees. Recognizing the impor-

tance of this certification program to both individuals' career development and to DoD mission readiness, the DoD CIO, in a May 2009 report to Congress on the DoD Civilian IT Workforce, recommended new legislation which would establish a Department-wide incentive program to encourage individuals to obtain key Cyber Security credentials.

A strong training program and consistently applied incentives, properly resourced, would separate DoD from its civilian counterparts during this recession. In a recent Gartner IT salary survey, 31% of the population surveyed indicated IT training budgets were dropping; another 58% reported their budget would be stagnant. Gartner cautioned that failure to adequately staff and develop IT personnel during this economic downturn could result in significant organizational turnover and loss of critical IT talent as the economy improves.

Mr. ANDREWS. What incentives does the DoD have to attract and retain quality skilled IT personnel? How do these incentives compare with the private sector?

Dr. NIELSEN. I'm happy to answer this based on my experiences in the government and since leaving the government. I'd like to make it clear that I am not speaking for the Department of Defense. In addition, I left government service in 2004 and I'm sure some personnel programs have changed since that time.

The largest incentive DoD has to attract and retain quality skilled IT personnel is that the work DoD does is important to our country. During my time as the commander of the Air Force Research Laboratory (2000–2004), we recruited scientists and engineers at all levels—men and women just completing their bachelors' degrees as well as senior, well-experienced, well-proven, professionals. Inevitably, they would mention a desire to serve their country as one of the key reasons, if not the primary reason, for why they joined our uniform or civilian workforce.

Among the more senior men and women who joined us, they would also mention the ability to shape and lead research and acquisition programs that were important to them professionally. By working for the government, they thought they could have more control over the direction of key programs and therefore have more impact to the country and their profession. In general, these individuals were very conscientious and hard working with clear ideas for the strategic impact of their work.

The government has been an especially good employer for scientific and technical men and women with respect to continuing education. The government supports the development of their IT personnel via short courses, attendance at professional conferences, and graduate education. These are all highly valued by IT personnel as well as all scientific and engineering professionals and lead to greater technical depth as well as technical and managerial breadth. This is true for both uniformed and civilian IT personnel.

DoD professionals also often cite the strong sense of mission and camaraderie as a reason for their continued service and retention. Often people think this is only true of the uniformed members, but throughout most of my career in research and development, most of my colleagues and subordinates were civilian government workers. I can say unequivocally that these civil service workers felt the same commitment to mission, the same dedication to their colleagues, the same passion for service to their country. I believe this plays a large role in retention of talented men and women who could have higher salaries elsewhere.

Having mentioned salaries, it is true, in general, that government salaries are not usually as high as industry salaries, especially for the top performers. Industry has more latitude on financial incentives—larger bonuses, stock and stock options—than the government has. In general, industry can advance top performers faster than the government can and this can be frustrating for a top performing government worker.

This has been addressed to some extent in the various personnel demonstration programs that have been authorized over the past 10–15 years. I am, of course, most familiar with the laboratory demonstration program implemented by the Air Force Research Laboratory in 1997. Instead of the well known civil service grades and steps, the civilian scientific and engineering workforce at AFRL was managed in four large groups with broad pay bands. Within broad guidance for overall salary growth, individuals were assessed annually on their contributions and their salary was adjusted based on the extent of their contributions. Under this system a new engineer who caught fire could receive substantial pay raises early in his or her career. Conversely, an individual who was not performing as expected might receive no raise at all, not even a cost of living adjustment—a clear sign that better performance was expected.

One topic I addressed in my oral testimony that relates to recruitment was the difference in the way the government and industry can respond to an applicant for a job. During my AFRL days, we occasionally lost a great applicant to industry because we could not make a firm offer as fast as industry could. When you're looking

for that first job or if you are an established IT professional who is looking for a career change, a quick and responsive offer might make the difference in which job you will accept. The government has improved its processes for making employment offers, but is usually not as quick and agile as industry is.

Overall, I believe DoD has the tools in place to recruit, retain, and develop its IT and acquisition workforces. It is a large and complex organization with a unique and challenging mission for our country. The expectations of the men and women it seeks to recruit and retain continue to evolve and, consequently, it must continue to evolve its processes to compete in the marketplace. It can do this through a thorough analysis of its work force goals, benchmarking against other organizations that manage their people well, and an honest assessment of its existing processes.

We ask our DoD IT and acquisition men and women to shoulder significant responsibilities and we need to reciprocate with the processes and infrastructure that support them.

Mr. ANDREWS. One of your recommendations is "selecting an effective leadership team." What are the critical skills or attributes needed by acquisition personnel overseeing IT programs? What questions should we be asking of leaders during the confirmation process to ensure we get the right people in key acquisition positions?

Dr. KERBER. These responses do not necessarily reflect the position of the Department of Defense and in some cases do not reflect the position of the Defense Science Board. I have tried to clearly identify those positions which are my own.

- A. The Department should select individuals that have exhibited proven success in leading and managing IT programs and acquisition or product development. Although DoD possesses a pool of talented individuals it does not have a sufficient number to meet all of its needs. DoD compensates for this shortfall with short assignments and inadequate screening of individuals by sometimes equating certification with competence. Certification can not be used as the sole factor for assigning an individual as a Program Manager. In my view, the private sector is the best model for finding this talent. The private sector encourages clear accountability and can only survive by having individuals that can develop and utilize state of the art technology. These two factors make it easy for the private sector to identify successful Program Managers. The Government often lacks clear accountability, drags programs on for years and therefore identifying the successful Program Manager becomes much more difficult.
- B. In addition to the traditional political vetting process, appointments should be accompanied with references of former supervisors and peers just like they are in the private sector. These references should include the typical areas such as leadership ability, teamwork skills, specific relevant key accomplishments, limitations, etc. Without references, one does not know if the experience listed by any potential employee, government or private sector, was successful or not.

Mr. ANDREWS. What incentives does the DoD have to attract and retain quality skilled IT personnel? How do those incentives compare with the private sector?

Dr. KERBER. The Department has many interesting and challenging programs to attract and retain quality skilled IT individuals. Quite often the work itself is so unique that it is its own incentive and DoD should do a better job of emphasizing the unique nature of its work. The Interagency Personnel Agreement (IPA) and other special programs for individuals of special talent are available that either offer monetary incentives or mobility. Our studies have shown that these programs are underutilized. Consistently our studies have shown that the best performance is when individuals have a lot of accountability and authority like at DARPA, Special Operations Command (SOCOM) or other special programs with small select staff.

I submitted 3 reports during my testimony. I would call your attention to a fourth DSB report "Management Oversight in Acquisition Organizations, March, 2005." This report covers topics associated with ethics in acquisition and other personnel issues. To acquire individuals with experience from the private sector, one by necessity needs to consider individuals that work in the industry that supplies the Department. While we all are concerned about improper behavior, corruption and revolving door issues, the private sector effectively manages these issues as people change companies sometimes moving from suppliers to procurers and from one competitor to the other. The Congress needs to remove onerous requirements placed on individuals moving from the private sector to government while keeping in place processes that prohibit one from making any decision that could impact their personal wealth or that of relatives and former colleagues. There is a large reservoir of recently retired, experienced and successful talent that is underutilized in the country.

When one compares the incentives for government service versus the private sector, for all but political appointees, job security is a big incentive. It is also a negative for the government since poor performers are hard and often impossible to remove. The positive incentives for individuals in the private sector are: 1) The customer can be clearly identified. 2) Decision authority is clearer and decisions are made relatively quickly and decisively. 3) Accountability is clearer. 4) Financial rewards are more closely tied to performance. 5) Incentives are clear. 6) Career planning is more interactive with the employer. Personal freedoms are encouraged and supported.

